HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

MASTERARBEIT

Frau B.A.
Julia Lutz

Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework mit besonderer Berücksichtigung der Änderungen in der Neuauflage 2013

Wien, 2014

Institut für Technologie- und Wissenstransfer

MASTERARBEIT

Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework mit besonderer Berücksichtigung der Änderungen in der Neuauflage 2013

Autor:
Frau B.A.

Julia Lutz

Studiengang:
Industrial Management

Seminargruppe:
ZM12wA2

Erstprüfer:
Prof. Dr. Johannes N. Stelling

Zweitprüfer:
Prof. Dr. Andreas Hollidt

Einreichung:
Wien, 20.November 2014

Verteidigung/Bewertung:
Mittweida, 2014

Institute for Technology and Knowledge Transfer

MASTER THESIS

Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework in special consideration of the changes in the new edition 2013

author:
Ms. B.A.

Julia Lutz

course of studies:
Industrial Management

seminar group:
ZM12wA2

first examiner:
Prof. Dr. Johannes N. Stelling

second examiner:
Prof. Dr. Andreas Hollidt

submission:
Vienna, 20.November 2014

defence/ evaluation:
Mittweida, 2014

Bibliografische Beschreibung:

Lutz, Julia:
Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework mit besonderer Berücksichtigung der Änderungen in der Neuauflage 2013. - 2014. – 14 Seiten Verzeichnisse, 84 Seiten Inhalt.
Wien, Hochschule Mittweida - University of Applied Sciences, Institut für Technologie- und Wissenstransfer, Masterarbeit, 2014

Referat:

In der komplexen Wirtschaftswelt von heute ist es für jedes Unternehmen von Bedeutung alle Risiken und Chancen zu erkennen und zu steuern. Dazu wurde, neben anderen, vom *Committee of Sponsoring Organizations of the Treadway Commission,* ein kompaktes und mittlerweile weltweit anerkanntes Kompendium zur Einführung eines internen Kontrollsystems entwickelt. Das **Internal Control - Integrated Framework** wurde erstmals im Jahr 1992 veröffentlicht und durch die richtungsweisenden Veränderungen in den letzten Dekaden im Jahr 2013 in einer neu überarbeiteten Version herausgegeben, um Unternehmen bei der Risikoerkennung in Bezug auf die Einhaltung von geltenden Gesetzen, Normen, Vorschriften und die Wahrung der sozialen Verantwortung des Unternehmens zu unterstützen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AAA	American Accounting Association
AAPA	American Association of Public Accountants
ACFE	Association of Certified Fraud Examiners
AIA	American Institute of Accountants
AICPA	American Institute of Certified Public Accountants
AS	Auditing Standard
Bzgl.	Bezüglich
Bzw.	Beziehungsweise
CCSA	Certification in Control Self Assessment
CEO	Chief Executive Officer
CFM	Certified Financial Manager
CFO	Chief Financial Officer
CFSA	Certified Financial Services Auditor
CGAP	Certified Government Auditing Professional
CIA	Certified Internal Auditors
CICA	Canadian Institute of Chartered Accountants
CMA	Certified Management Accountant
COBIT	Control Objectives for IT and related Technology
CoCo	Criteria on Control
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountant
CRMA	Certification in Risk Management Assurance
ERM	Enterprise Risk Management
FCPA	Foreign corrupt Practices Act

FEI	Financial Executives Institute
IC	Internal Control
IIA	Institute of Internal Auditors
IMA	Institute of Management Accountants
IPPF	International Professional Practices Framework
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
No.	Number
PCAOB	Public Company Accounting Oversight Board
QIAL	Qualification in Internal Audit Leadership
RMS	Royal Mail Ship
SAS	Statement on Auditing Standards
SEC	Securities and Exchange Commission
Sec.	Section
SOX	Sarbanes-Oxley Act
US	United States
USA	United States of America
Usw.	Und so weiter

1 Einleitung

„W*enn mich jemand fragt, wie ich am besten meine Erfahrungen aus 40 Jahren auf hoher See beschreiben würde, so könnte ich diese Frage lediglich mit unspektakulär beantworten. Natürlich gab es Stürme, Gewitter und Nebel, jedoch war ich nie in einen Unfall jeglicher Art verwickelt, der es wert wäre, über ihn zu berichten.*“[1]

Ein oft zitierter Ausspruch des Luxusschiffkapitäns der *RMS Titanic* Edward John Smith (*27.01.1850 †15.04.1912), datiert auf das Jahr 1907, hat bereits gezeigt, dass bei jeder Unternehmung die Risiken, die diese mit sich bringen kann, nicht zu ignorieren sind. Denn am 14. April 1912 raste die *RMS Titanic* bei ihrer Jungfernfahrt mit überhöhter Geschwindigkeit frontal gegen einen Eisberg. Das blinde Vertrauen, das dem Kapitän entgegengebracht wurde, vor allem wegen seiner perfekten Ausstrahlung und seiner Immunität gegen Kritik und den Ruf des Schiffes, durch neueste Sicherheitskonzepte unsinkbar zu sein, ohne vorab Tests durchzuführen oder präventive Maßnahmen zu ergreifen, aber auch die Ignoranz gegenüber allen Frühwarnindikatoren, wie Eisbergwarnungen per Telegramm und Funk, führten zu diesem verheerenden Unglück.[2]

Diese plakative Darstellung eines geschichtlichen Ereignisses lässt sich mit der komplexen Wirtschaftswelt des 21. Jahrhunderts vergleichen, in der etablierte Unternehmen Risiken zu spät erkennen, Frühwarnindikatoren ignorieren oder korrupt handeln. Um diesem Umstand Rechnung zu tragen, ist es umso bedeutender, für jedes Unternehmen alle Risiken und auch Chancen zu erkennen und zu steuern. Abgesehen von den gesetzlichen Regelungen, welche national und teilweise international zum Tragen kommen, wurde, neben anderen, von einer gemeinsamen Initiative von fünf privaten Organisationen, dem *Committee of Sponsoring Organizations of the Treadway Commission,* ein kompaktes und mittlerweile, durch die Zitierung der Securities and Exchange Commission, weltweit anerkanntes Kompendium zur Einführung eines internen Kontrollsystems entwickelt. Das **Internal Control - Integrated Framework** wurde erstmals im Jahr 1992 veröffentlicht und durch die richtungsweisenden Veränderungen in den letzten Dekaden im Jahr 2013 in einer neu überarbeiteten Version herausgegeben, um Unternehmen bei der Risikoerkennung in Bezug auf die Einhaltung von geltenden Gesetzen, Normen, Vorschriften und die Wahrung der sozialen Verantwortung des Unternehmens zu unterstützen.[3]

---

[1] Romeike/Hager 2009, S.283.
[2] Vgl. Romeike/Hager 2009, S.283f.
[3] Vgl. im Folgenden Arwinge 2013, S.43.; Moeller2014, Chapter 3 (e-book) und Romeike/Hager 2009, S.283f.

2 Internal Control

In der heutigen Zeit müssen Unternehmen mit einer immer schneller wachsenden und sich verändernden Ökonomie leben, in der es verständlich ist, dass eines der Hauptziele im Unternehmen der Profit ist. Dabei gilt, wie in allen Bereichen: je größer der mögliche Profit ist, desto größer ist auch das Risiko. Um dieses Risiko einzugrenzen und zu steuern, ist eine der wichtigsten Entscheidungen des Topmanagements die für ein internes Kontrollsystem, welches die Ziele und Werte eines Unternehmens widerspiegelt und somit die Haltung aller involvierten Personen beeinflusst. Vor allem in operativen Tätigkeiten steigt die Komplexität der Zusammenhänge, und es kommt nur in den wenigsten Fällen zu Abweichungen durch Vorsatz, vielmehr sind es in der Regel die Änderungen in den externen Bedingungsgefügen, damit lässt sich die Transparenz und Ordnungsmäßigkeit schwer erfüllen. Ein Unternehmen bedient sich demnach Vorkehrungen wie dem Controlling, welches explizite ergebnisrelevante Daten liefert und gestaltet, und eines Gerüsts zur Aufbau- und Ablauforganisation, welches durch eine Vielzahl detaillierter Regelungen konkret ausformuliert wird. Diese Regelungen werden in der Gesamtheit als internes Kontrollsystem bezeichnet.[4]

2.1 Definition von Internal Control

Der Begriff Internal Control verbindet im Englischen das Wort *internal* oder intern, also im engeren Sinn die Arbeitsabläufe integrierter oder damit verbundener Maßnahmen innerhalb bestimmter Grenzen, wobei diese auch externe Elemente umfassen kann, soweit diese in einem Verhältnis zu den Arbeitsabläufen oder der Struktur stehen, und das Wort *control* oder Kontrolle. Das Wort *control* ist auf den französischen Begriff *contre-rôle* zurückzuführen, welches im weiteren Sinn das Führen eines Zweitregisters zur Prüfung der Richtigkeit eines Originalregisters bedeutet und in der englischen Sprache als Substantiv einen erreichten Zustand beschreibt. Als Verb *to control*, also die Kontrolltätigkeit, wird es als kontinuierlicher Prozess angesehen, mit welchem ein System oder ein anderer Prozess in ständiger Wechselwirkung gesteuert und kontrolliert wird, um damit die Zielerreichung sicherzustellen, indem bereits vorliegende Mängel aufgedeckt, korrektive Maßnahmen eingeleitet, unerwünschte Ereignisse verhindert und gewünschte Zustände gestaltet und gefördert werden.[5] Zusammenfassend kann gesagt werden, dass „Internal Control alles umfasst, was zu einer organisierten Struktur (…) gehört und darauf ausgerichtet ist, Ereignisse, welche die Erreichung der Ziele beeinträchtigen könnten, zu steu-

[4] Vgl. im Folgenden COSO1994, S.24 und Euler1992, S12.
[5] Vgl. Im Folgenden Jenal2006, S.2 und Root1998, S.22.

ern und zu kontrollieren, sowie diese Steuerung und Kontrolle zu prüfen und zu überwachen.“[6] Diese Definition des Begriffs Internal Control ist in keinem Lexikon zu finden, da beide Wörter nur einzeln definiert werden. Festgehalten werden kann jedoch, dass durch die gestiegene Bedeutung der Internal Control, durch die ständig zunehmende Komplexität des Umfelds für Unternehmen und durch den Zusammenbruch einiger großer Unternehmen, welche teilweise auf Kontrollschwächen zurückzuführen sind, einige regulatorische Bestimmungen, theoretische und praktische Rahmenwerke und andere Publikationen veröffentlicht wurden, welche ein teilweise differenziertes Grundverständnis in ihrer Definition bieten. Zu den wichtigsten international gültigen Regulierungen gehört der *Sarbanes-Oxley Act* (SOX) und darin besonders die Sektion 404 *Management Assessment of Internal Control* für die Gestaltung von internen Kontrollen über die Finanzberichterstattung von Unternehmen, verpflichtend für Unternehmen, welche an einer amerikanischen Börse notiert sind.[7]

Diese Regelung beschränkt sich jedoch auf die Finanzberichterstattung und umfasst nicht die Bereiche „*Compliance*“, „*Operations*“ und „*Strategy*“, die als Teil der zu erfüllenden Mindestanforderungen für ein geeignetes und anerkanntes Internal-Control-Rahmenwerk festgelegt sind. Diese Mindestanforderungen wurden von der durch SOX ins Leben gerufenen Aufsichtsbehörde *Public Company Accounting Oversight Board* (PCAOB), im *Auditing Standard* (AS) No.2 bzw. infolge von AS No.5 definiert und empfiehlt das *Committee of Sponsoring Organizations (COSO) Internal Control – Integrated Framework* „*which provides a suitable and available framework for purposes of management's assessment. (…) Although different frameworks may not contain exactly the same elements as COSO, they should have elements that encompass, in general, all the themes in COSO.*“[8]

Durch diese Festlegung kann davon ausgegangen werden, dass die Definition nach COSO, in der Internal Control als Prozess zur Erreichung von Zielen ausgerichtet ist, von Menschen durchgeführt wird, eine angemessene Sicherheit gewährleistet und an jede Unternehmensstruktur angepasst, als allgemeingültig angesehen werden kann und damit vor allem die Zielkategorien zur Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit, Ordnungsmäßigkeit und Verlässlichkeit der Berichterstattung, Einhaltung von Gesetzen und Vorschriften abdeckt.[9]

[6] Jenal2006, S.3.
[7] Vgl. im Folgenden Sommer2010, S.20 und Löffler2011, S.570ff.
[8] PCAOB2003-2014, AS2 (14).
[9] Vgl. im Folgenden Löffler2011, S.572f. und COSO2013, S.1ff.

2.2 Begriffe zum Internal Control

2.2.1 Internes Kontrollsystem

Im Gegensatz zu dem Wort Internal Control, welches in dieser Zusammensetzung in keinem Lexikon zu finden ist, gibt es zum Internen Kontrollsystem, oder auch Internen Überwachungssystem eine Vielzahl von Einträgen, von denen die meisten ebenfalls auf die Definition der Internal Control nach COSO verweisen. Festzuhalten ist jedoch, dass jedes Unternehmen, innerhalb der definierten Struktur, die Verlässlichkeit und Ordnungsmäßigkeit der Funktionsabläufe durch vordefinierte Systeme sicherstellen sollte und damit das Geschehen im Unternehmen an jeder Stelle transparent macht. Die Ausgestaltung einer Aufbau- und Ablauforganisation mit detaillierten Regeln und Arbeitsanweisungen definiert dabei den organisatorischen Rahmen eines Unternehmens und bietet außerhalb von konkreten ergebnisrelevanten Daten zur unmittelbaren erfolgsorientierten Überwachung die Möglichkeit, die Ordnungsmäßigkeit und Transparenz im Unternehmen sicherzustellen. Die Gesamtheit dieser internen Regelungen wird als internes Kontrollsystem bezeichnet, da ein unmittelbarer zielorientierter Vergleich zwischen einem Sachverhalt und einem Vergleichsobjekt, also dem Soll-Zustand und dem Ist-Zustand, ermöglicht wird, um sicherzustellen, dass „die Sicherung der betrieblichen Vermögenswerte, die effiziente Gestaltung betrieblicher Abläufe, die Einhaltung der von der Unternehmensleitung vorgegebenen Leitlinien zur Geschäftspolitik und (…) die Verlässlichkeit und Genauigkeit des Rechnungswesens“[10] gegeben sind. Während dieses Vergleichs können Fehler verhindert oder bereits passierte Fehler dokumentiert werden, um eine Erreichung von vorab definierten Unternehmenszielen so gut wie möglich zu sichern. Dabei wird zwischen prozessunabhängigen Vergleichen bzw. Kontrollen, welche von Personen, Personengruppen und Institutionen durchgeführt werden, welche nicht direkt mit dem zu überprüfenden Prozess in Zusammenhang stehen, und prozessabhängigen Vergleichen, die von Personen, in einem direkt Verhältnis mit dem zu überprüfenden Prozess stehen, durchgeführt werden, unterschieden.[11]

Damit kann das Interne Kontrollsystem, neben den unmittelbaren ergebnisrelevanten und erfolgsorientierten Überprüfungen als die Gesamtheit aller prozessbezogenen Überwachungsmaßnahmen einer Organisation bezeichnet werden und soll damit

- „die ordnungsgemäße Geschäftsführung,
- die Einhaltung der Geschäftspolitik,
- die Einhaltung gesetzlicher und sonstiger rechtlicher Grundlagen (Compliance),
- die Einhaltung vorgegebener Ziele,
- die Vermögenswerte der Organisation,

[10] Horvath2003, S.315.
[11] Vgl. im Folgenden Horvath2003, S.315ff. und Euler1992, S.12.

- die Vollständigkeit und Zuverlässigkeit von Informationen, Dokumentationen und Prozessen,
- die Wirtschaftlichkeit und Effektivität von Prozessen,
- die Verhütung und Entdeckung von Fehlern und Unregelmäßigkeiten und
- die Transparenz und Nachvollziehbarkeit von Abläufen zum Schutz der Prozessbeteiligten (…)“[12]

sicherstellen und unterstützen. Die Verantwortung für die Einführung des Internen Kontrollsystems liegt bei der Geschäftsführung bzw. ist Teil der Führungsverantwortung und beginnt, wie bereits oben beschrieben, mit dem Aufbau einer transparenten Aufbauorganisation, die durch explizite Funktionsbeschreibungen eine klare Kompetenzabgrenzung und konsequente Funktionstrennung sicherstellt, die die Entscheidung vom Vollzug der Kontrollen per Definition zu einer Trennung führen kann. Das COSO – Internal Control Framework spricht weiter von „*tone at the top*“ und beschreibt auf Basis dieser Vorgaben einen Teil der Führungsverantwortung mit den Erwartungen, die außerhalb der lokalen Gesetzgebung und Normen im Unternehmen gelebt werden und bei komplexen Situationen oder schwierigen Entscheidungen als Vorbildwirkung die Betroffenen beeinflusst, sodass die Umsetzung durch jeden Mitarbeiter den Zweck eines Internen Kontrollsystems in der Gesamtheit des Prozesses mit der Steuerung von Zielen sicherstellt, um die Häufigkeit und die Auswirkungen von Fehlern auf ein steuerbares Niveau zu bringen.[13]

„*The principal conceptual foundation of internal control is the perceived inseparable relationship between the action of controlling and its objective: being in control*.”[14]

2.2.2 Risikomanagement

Risikomanagement ist ein prozessabhängiger Teil der Kontrollfunktionen in einem Unternehmen. In den letzten Jahrzehnten hat sich das Gebiet von finanziellen Versicherungslösungen und vor allem von deren Auswirkungen auf die Erreichung von Unternehmenszielen, welchen mit Ad-hoc-Reaktionen auf einzelne Ereignissen entgegengewirkt wurde, zu einem Risikomanagement in weiterem Fokus, welches alle relevanten Risiken miteinschließt, entwickelt. Es setzt sich mit schadensverursachenden Risiken und auch gewinnversprechenden Chancen auseinander und besteht aus:

- Der **Risikopolitik**, also der Festlegung der Geschäftsführung im Umgang mit Risiken, ist ein wesentlicher Teil der Geschäftspolitik jeder Organisation und deren Aufgabe, besteht in der Absicherung der wirtschaftlichen, sozialen und finanziellen Ziele mit der Dokumentation der unternehmerischen Grundsätze zum Risikomanagement.

---

[12] IIA2004, S.18.
[13] Vgl. im Folgenden Root1998, S.25; COSO2013, S.33f.; CFOaktuell2010_25, S.1 und Huska1996, S.10f.
[14] Root1998, S.25.

- Das **Früherkennungssystem** umfasst quantitative und qualitative Instrumente, die zur Aufdeckung, Steuerung und Bereinigung von noch nicht realisierten, neuen oder weggefallenden Risiken und Chancen dienten und die aktuelle Entwicklung abdecken.
- Das **operative Risikomanagement** ist die Überleitung zum Internen Kontrollsystem und stellt alle Maßnahmen dar, welche zur Reaktion auf Risiken und Chancen zum Beispiel im personellen, organisatorischen, technischen oder kommunikativen Bereich erfolgen.[15]

Daraus kann abgeleitet werden, dass das Risikomanagement und Internal Control eng verknüpft sind, da eine wirksame Internal Control risikoorientiert ist und auf die Steuerung von Risiken ausgerichtet ist, die im Rahmen des Risikomanagements identifiziert und beurteilt werden. Umgekehrt bedarf ein wirksames Risikomanagement einer effektiven Internal Control, um die identifizierten Risiken zu steuern und die Umsetzung der im operativen Risikomanagement definierten Maßnahmen sicherzustellen. Vor allem nach der Veröffentlichung des Regelwerks *COSO Internal Control – Integrated Frameworks* (*COSO IC*) zur Gestaltung eines Internen Kontrollsystems wird die Wichtigkeit für ein unternehmensweites Risikomanagementsystem deutlich. Aufgrund dessen wird das *COSO Enterprise Risk Management – Integrated Framework* (*COSO ERM*) im Jahr 2004 veröffentlicht. Das *COSO ERM* ist eine Weiterentwicklung des *COSO IC* und macht damit deutlich, dass das Interne Kontrollsystem ein Bestandteil eines unternehmensweiten Risikomanagementsystems ist. Das COSO ERM ist definiert als „*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*"[16] und baut auf den Grundsätzen des Internal Control auf, ergänzt um risikobezogene Aspekte. Vergleicht man die Zieldimensionen, so beinhaltet das COSO IC Modell Operative-, Compliance- und Finanzberichterstattungs-Ziele; anstelle letzter Zielkategorie tritt im COSO ERM die umfassende Berichterstattungsziel- Kategorie, die sowohl monetäre als auch nichtmonetäre Berichterstattung beinhält. Zudem gibt es eine weitere Zielkategorie, die den bereits genannten Zielen übergeordnet ist und eine langfristige Kategorie darstellt: die strategischen Ziele. Auch die fünf Dimensionen des Internal-Control-Modells wurden im Enterprise-Risk-Management-Modell auf acht Dimensionen erweitert, obwohl diese Erweiterung in Bezug auf den Inhalt eher als Umstrukturierung zu verstehen ist, da die Komponente Risikobeurteilung in die vier Bestandteile, Zielsetzungsprozess, Ereignisidentifikation, Risikobeurteilung und Risikohandhabung unterteilt wird.[17]

---

[15] Vgl. im Folgenden Sommer2010, S.18 und IIA2004, S.23f.
[16] COSOERM2004, S.2.
[17] Vgl. im Folgenden Brünger2009, S.18ff.; Sommer2010, S.23f. und Peemöller2010, S.87ff.

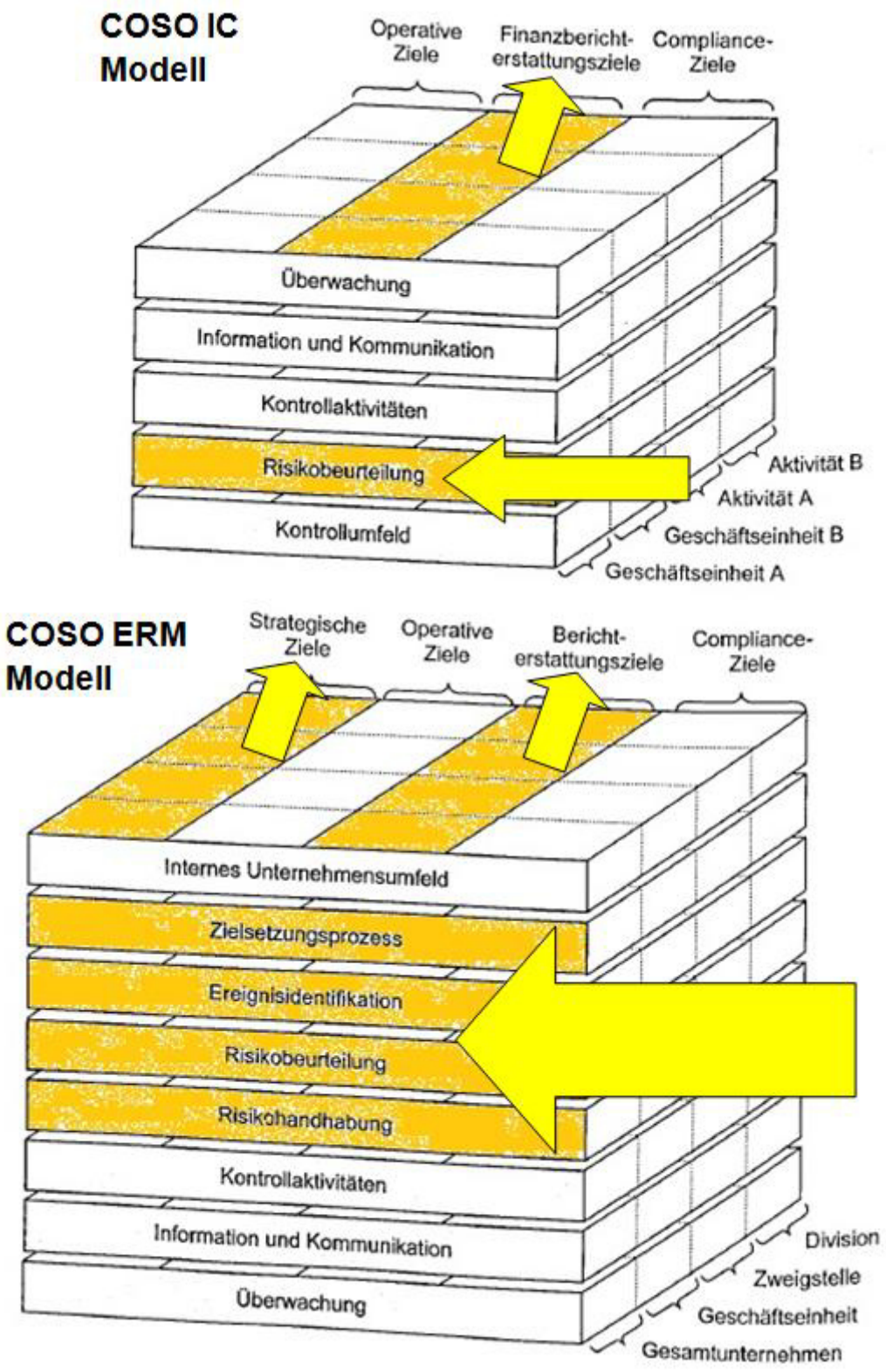

Abb. 1 COSO IC Modell erweitert zum COSO ERM Modell[18]

[18] Vgl. Brünger2009, S.20.

Eingehend auf die Rahmenbedingungen, die sich ausschließlich auf das COSO ERM beziehen, muss ein Unternehmen zur Identifizierung von Risiken zuerst die Ziele kennen, welche potenziell gefährdet sein können. Diese Komponente ist Teil des Risikomanagements, da die Vereinbarkeit der strategischen, operativen, Berichterstattungs- und Compliance-Ziele die Risikobereitschaft und Toleranzgrenzen sicherstellen und damit den Ausgangspunkt bilden (*Objective Setting*). Mit der Festlegung der Ziele können alle Ereignisse, sowohl externe als auch interne negative und positive Faktoren bzw. Abweichungen, identifiziert werden, die eine Auswirkung auf die Zielerreichung haben können. Diese Identifizierung soll unternehmensweit stattfinden und muss anhand von Grundsätzen, Richtlinien und dem Verfahren der Geschäftsführung an die Mitarbeiter weitergegeben werden, um das Ergebnis in festgelegten Intervallen zusammenzufassen (*Event Identification*). Im Anschluss werden die erfassten Risiken und Chancen anhand der Eintrittswahrscheinlichkeit und der Höhe der qualitativen und quantitativen Auswirkung auf das Ergebnis bewertet und mit einem zeitlichen Planungshorizont eingeordnet. Diese Risikobeurteilung (*Risk Assessment*) muss ganzheitlich erfolgen, um die Wechselbeziehung zwischen den einzelnen Risiken und Chancen erkennen zu können. Bei der Handhabung der identifizierten und bewerteten Risiken (*Risk Response*) werden in einem ersten Schritt Maßnahmen festgelegt, die in folgende vier Kategorien eingeteilt werden können[19]:

- Risikovermeidung (*Avoidance*), durch Verzicht auf die risikobelastete Tätigkeit,
- Risikoreduktion (*Reduction*), durch Einleitung von Maßnahmen zur Reduktion des Risikos,
- Risikoteilung (*Transfer*), durch einen Transfer des Risikos an Dritte und
- Risikoübernahme (*Acceptance*), durch das bewusste Nichthandeln.[20]

Diese Maßnahmen werden in einem zweiten Schritt so formuliert, um das Niveau des Risikos auf ein in den Toleranzgrenzen liegenden Bereich zu reduzieren, und werden anhand einer Gegenüberstellung von Kosten und Nutzen beurteilt. Sicherzustellen ist bei jeder Maßnahme, den Einfluss auf das gesamte Risikoportfolio zu kennen und zu berücksichtigen, um die gesamte Unternehmenszielerreichung nicht zu gefährden und entsprechend der Risikobereitschaft des Unternehmens zu handeln. Zusammengefasst werden kann, dass das Enterprise Risk Management und das Internal Control in einem Unternehmen klar formulierte Strategien und ein starkes Engagement voraussetzen, das von der obersten Führungsebene kommuniziert werden muss und damit die Bedeutung verdeutlicht. Nur so kann ein konsequenter Ansatz genutzt und im täglichen Geschäftsablauf für die Entscheidungsfindung und Unternehmenskultur wirksam sein.[21]

[19] Vgl. im Folgenden Sommer2010, S.79f. und Menzies2004, S.119ff.
[20] Vgl. Sommer2010, S.80.
[21] Vgl. im Folgenden Menzies2004, S.120ff. und Sommer2010, S.80.

2.2.3 Sarbanes-Oxley Act

"*An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for the purposes.*"[22]

Der *Sarbanes-Oxley Act of 2002* (*SOX*) ist Teil der US-amerikanischen Gesetzgebung, verpflichtend für alle an amerikanischen Börsen notierte inländische und ausländische Unternehmen. Primär wurde der SOX verabschiedet, um die Finanzberichterstattung börsennotierter Unternehmen zu verbessern und das Vertrauen der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichen Finanzdaten zu sichern. Diese Ziele sollen vor allem durch genauere und verlässlichere Publizitätspflichten nach außen erreicht und innerhalb des Unternehmens durch eine Qualitätssicherung der Unternehmensführung und die Transparenz der Unternehmensprozesse sichergestellt werden. Der *Sarbanes-Oxley Act* enthält elf Rubriken, mit Bestimmungen und Verordnungen, die einen Einfluss auf Unternehmen, deren Management und externe Wirtschaftsprüfer hat, zu welchen in Bezug auf Internal Control vor allem der Absatz (Sec.) 404 und Sec. 302 von Bedeutung sind.[23]

„I Public Company Accounting Oversight Board
Festlegung von Organisation und Aufgabenbereich des Aufsichtsratsgremiums über die Abschlussprüfung (…)

II Auditor Independence
Bestimmungen zur Unabhängigkeit der Wirtschaftsprüfer

III Corporate Responsibility
Erläuterung und Erweiterung der Verantwortlichkeiten der einzelnen Unternehmen

IV Enhanced Financial Disclosures
Festlegung von erweiterten Veröffentlichungspflichten für Finanzinformationen

V Analyst Conflicts of Interest
Vorschriften zur Verhinderung von Interessenkonflikten der Finanzanalysten

VI Commission Resources and Authority
Einzelregelung bzgl. Finanzierung und Befugnissen der SEC

VII Studies and Reports
Festlegung der Themen, zu denen US-Behörden Studien und Berichte zu erstellen haben

[22] Holt2006, S.3.
[23] Vgl. im Folgenden Burger2012, S66 und Peemöller2010, S.70f.

VIII Corporate and Criminal Fraud Accountability
Regelungen zum Informationsschutz und zu den erweiterten Aufbewahrungspflichten für Dokumente

IX White – Collar Crime Penalty Enhancements
Verschärfung der strafrechtlichen Bestimmungen bei unrichtiger eigenstaatlicher Bestätigung

X Corporate Tax Returns
Festlegung zur Unterzeichnung der Steuererklärung durch den CEO

XI Corporate Fraud and Accountability
Bestimmungen zur Verantwortlichkeit der Geschäftsleitung im Falle von Unregelmäßigkeiten"[24]

Zusammengefasst kann gesagt werden, dass die wichtigsten Aspekte von SOX im Bestreben nach Sicherheit, in der Formalisierung und Stärkung von Corporate Governance, durch die Aufstellung von Regeln für die Unternehmensleitung und externe Prüfer sowie in der Sicherstellung der Unabhängigkeit der Wirtschaftsprüfer gegenüber dem Kundenunternehmen und in der Stärkung der Bedeutung von ethischen Standards in Unternehmen, ausformuliert sind. Einige wesentlichen Regelungen betreffen damit zum Beispiel die Rückzahlung erfolgsabhängiger Vergütungen im Falle von unrichtigen Abschlüssen, das Verbot der Darlehensgewährung an die Geschäftsführung, eine erweiterte finanzielle Offenlegungspflicht und die Verschärfung der Strafvorschriften. SOX enthält damit Bestimmungen und Verordnungen, die einen Einfluss auf alle Zielgruppen im Unternehmen und deren externe Prüfer haben und tangiert vor allem verschiedene Aspekte der Compliance, der Corporate Governance und der Berichterstattungspflichten von Kapitalgesellschaften sowie der damit zusammenhängenden Durchsetzung.[25]

In engem Zusammenhang mit SOX in Bezug auf Internal Control steht die Sec. 302, „wonach Unternehmen eine vollständige und richtige Veröffentlichung aller erforderlichen Informationen gewährleisten müssen und dies durch eine eidesstattliche Erklärung (*Certification*) des CEO und CFO zu bestätigen haben"[26]. Um diese Erfordernisse einzuhalten, müssen in einem Unternehmen Kontrollen identifiziert werden, die eine genaue und vollständige Offenlegung von Unternehmensdaten gewährleisten, da die Folgen falscher Angaben in der Finanzberichterstattung oder eine Nichtunterzeichnung laut SOX zwischen fünf Millionen Dollar und einer 20-jährigen Gefängnisstrafe liegen kann. Ein weiterer wichtiger Teil der Sec. 3 im Abschnitt (a) ist die Ermächtigung der *Securities and Exchange Commission* (SEC), weitere Ausführungsbestimmungen zu allen im SOX enthaltenen Regelungen zu erlassen, diese betreffen vor allem Konkretisierungen und Ausnahmerege-

[24] Burger2012, S.66 und 67.
[25] Vgl. im Folgenden Giller2008, S.15ff. und Burger2012, S.68.
[26] Welge2012, S.47.

lungen oder auch verlängerte Umsetzungsfristen für bestimmte Unternehmensgruppen. „Vorschriften und Prüfungsstandards für den Abschlussprüfer des SOX werden durch das PCAOB erarbeitet, wobei deren endgültige Verabschiedung jedoch der SEC obliegt.“[27] Wie bereits in Kapitel 2.1 beschrieben, wurden auch die Mindestanforderungen für ein geeignetes und anerkanntes Internal-Control-Rahmenwerk von der PCAOB im AS No.2 bzw. in Folge AS No.5 definiert und empfiehlt das COSO Internal Control – Integrated Framework zur Erfüllung des SOX Sec. 404.[28]

„***SOX Sec. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS:***

(a) RULES REQUIRED. – The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (…) to contain an internal control report, which shall -

(1) State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.

(2) Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING. – With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.”[29]

In diesem Absatz des SOX wird die Einführung eines Internal-Control-Systems verlangt, um jeden Aspekt der Unternehmenstätigkeiten mit Einfluss auf die Finanzberichterstattung abzudecken und über ausreichend Möglichkeiten zur Erstellung von umfassenden und transparenten Berichten zu verfügen. Die Umsetzung der Sec. 404 wird in verschiedenen Leitfäden und Anforderungen der SEC und dem PCAOB beschrieben und kann demnach in drei Phasen zur Implementierung aufgeschlüsselt werden: In der ersten Phase (*Scoping Phase*) muss zuerst die Anzahl der signifikanten Konten identifiziert werden; nach dem PCAOB ist ein Konto insofern signifikant, als es Fehler aufweisen soll, die einen wesentlichem Einfluss auf die Finanzberichterstattung haben. Im Anschluss werden alle signifikanten Unternehmenseinheiten oder Standorte identifiziert, in der Regel werden alle Niederlassungen, welche eine bestimmte Grenze überschreiten, unternehmensintern

[27] Lück2009, S.157.
[28] Vgl. im Folgenden Giller 2008, S.18; Löffler2011, S.573; Lück2009, S.157 und Welge2012, S.47.
[29] SOX2002, S.45, 116 –Stat. 789; 15 USC 7262.

SOX pflichtig. Als letzter Schritt werden alle signifikanten Prozesse identifiziert, also Geschäftsprozesse, welche finanzrelevante Daten betreffen und in Bezug auf signifikante Konten oder die Finanzberichterstattung relevant sind. Die zweite Phase (*Documentation Phase*) ist die für ein Unternehmen kostenintensivste Phase, in der ein Internal-Control-System aufgebaut und dokumentiert werden muss. In der letzten Phase (*Validation Phase)* werden der Aufbau und die operative Wirksamkeit der internen Kontrollen sowie der formellen Berichterstattung von Fehlern und deren Maßnahmen zur Verbesserung vor dem endgültigen Abschluss der Geschäftsführung durch die Zertifizierung geprüft. Damit soll mit der Entwicklung eines internen Kontrollsystems über die Finanzberichterstattung nach SOX Sec. 404 die Geschäftsführung dabei unterstützt werden, Fehler und Betrug zu erkennen, zu vermeiden und zu beseitigen, um sich auf die Daten in der Finanzberichterstattung verlassen zu können.[30]

[30] Vgl. im Folgenden Giller2008, S.29ff. und Holt2006, S.34.

2.3 Internal-Control-Modelle

2.3.1 Committee of Sponsoring Organizations of the Treadway Commissions

Die Organisation *Committee of Sponsoring Organizations of the Treadway Commission* (*COSO*) wurde Mitte der 1980er Jahre von der *American Association*, dem *Institute of Internal Auditors*, dem *Financial Executive Institute* und dem *Institute of Management Accountants* als unabhängige nationale Kommission ins Leben gerufen, um die Kommission gegen betrügerische Absichten bei der Finanzberichterstattung (*US Foreign Corrupt Practices Act – FCPA*) zu unterstützen. Im Zuge dieser im privaten Sektor angesiedelten Initiative wurden elf Empfehlungen veröffentlicht, welche den Grundstein für die heute bekannte *Corporate Financial Governance* legten. Im Jahr 1992 wurde erstmalig der *COSO* – Report *Internal Control – Integrated Framework* als Leitlinie zum Aufbau und zur Beurteilung von Internen Kontrollsystemen veröffentlicht. Mit dieser Studie sollen die verschiedenen internen Kontrollbegriffe vereinheitlicht und Normen aufgestellt werden, mit denen ein Unternehmen in der Lage sein soll, die internen Kontrollsysteme auf ihre Wirksamkeit zu prüfen. Diese Studie besteht aus vier Teilen – die Kurzdarstellung, das Framework, der Bericht zur Berichterstattung an Dritte und das Kompendium zu Evaluierungsinstrumenten – und wurde im Laufe der Jahre teilweise angepasst. Nachdem von der amerikanischen Börsenaufsicht der *Sarbanes-Oxley Act* (*SOX*) für in den USA börsennotierte Unternehmen anerkannte Kontrollsysteme vorgeschrieben wurden und im Jahr 2004 eine Adaptierung des *COSO* Frameworks um den umfassenden Teil *Enterprise Risk Management* (*ERM*) erfolgte, wurde das *COSO*-Modell vor allem von amerikanischen Unternehmen und Wirtschaftsprüfern als Framework anerkannt und wird inzwischen weltweit eingesetzt. Im Jahr 2013 wurde eine Neuauflage des „*Internal Control – Integrated Framework*“ herausgegeben, um die bereits über 20 Jahre alte Version auf den neuesten Stand des Wissens anzupassen. [31]

Das *COSO Internal Control – Integrated Framework* beinhaltet Definitionen und einen umfassenden Leitfaden zu internen Kontrollen, mit dem vor allem Auditoren, Manger, Prüfungsausschüsse und Aufsichtsbehörden angesprochen werden. Es werden umfassende Standards aufbereitet, mit welchen eine Organisation das eigene Interne Kontrollsystem überprüfen und, wenn notwendig, einen Ausbau oder eine Verbesserung erarbeiten kann.[32]

[31] Vgl. im Folgenden Arwinge2013, S.39; Burger2012, S.88f.; Arwinge2013, S.39 und Klinger2011, S.18.
[32] Vgl. Arwinge2013, S.39.

2.3.2 Canadian Institute of Chartered Accountant's Criteria of Control Framework

Das *Canadian Institute of Chartered Accountants* (CICA), ist eine Non-Profit-Organisation, die vom kanadischen Parlament im Jahr 1902 ins Leben gerufen wurde und heute eine Vereinigung von mehr als 80.000 Wirtschaftsprüfern umfasst, sie hat sich "*supporting the setting of accounting, auditing and assurance standards for business, not-for-profit organizations and government; developing and delivering pre- and post-qualification education programs, providing a range of member services and professional literature, research and development of intellectual property, issuing guidance on risk management and governance and fostering relationships with key stakeholders nationally and internationally*"[33] zur Aufgabe gemacht. Neben dem COSO Framework hat das CICA das anerkannteste Internal Control Framework, *Criteria on Control* (CoCo) herausgegeben, in dem ein Verständnis für Internal Control durch die Beschreibung von zwanzig Kriterien für effektive Kontrollen und deren Einordnung in vier Gruppen gegeben werden sollen[34]:

1. „***Purpose*** *– The criteria in this group provide a sense of the organization's direction and relate to these objectives:*
    a. *Mission, vision, and strategy.*
    b. *Risk and opportunities*
    c. *Policies.*
    d. *Planning.*
    e. *Performance targets and indicators.*
2. ***Commitment*** *– The criteria in this group provide a sense of the organization's identity and values and pertain to ethical values, including:*
    a. *Integrity.*
    b. *Human resource policies*
    c. *Authority, responsibility, and accountability.*
    d. *Mutual trust.*
3. ***Capability*** *– The criteria in this group provide a sense of the organization's competence and address:*
    a. *Knowledge, skills, and tools.*
    b. *Communication processes.*
    c. *Information.*
    d. *Coordination.*
    e. *Control activities.*

[33] CICA2013, „Incorporation and Governance".
[34] Vgl. im Folgenden CICA2013, „About"; Pickett2010, S.264ff. und Sonnelitter2009, S.1.15.

4. ***Monitoring and learning*** *– The criteria in this group provide a sense of the organization's evolution and address:*
    a. *Monitoring internal and external environments.*
    b. *Monitoring performance.*
    c. *Challenging assumptions.*
    d. *Reassessing information needs and information systems.*
    e. *Follow-up procedures.*
    f. *Assessing the effectiveness of control.*"[35]

Sowohl das COSO-Modell als auch das CoCo-Modell zu Internal Control bieten einen guten Rahmen für die Entwicklung eines Internal-Control-Systems in einem Unternehmen, wobei das COSO-Modell sich auf die wichtigsten Strukturen, Werte und Prozesse in einem Unternehmen konzentriert und der Fokus des CoCo-Frameworks stark auf jedes einzelne Individuum als Teil des Gesamtprozesses abzielt; so ist das CoCo-Modell stärker auf eine Lernkurve fokussiert, welches damit Teams und Einzelpersonen besser ansprechen soll.[36]

2.3.3 Control Objectives for Information and Related Technology

"*Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments.*"[37]

Basierend auf dem COSO-Modell zum Internal Control, wurde von der *Information Systems Audit and Control Association* (ISACA) ein Governance- und Kontrollmodell speziell für Informationstechnologie veröffentlicht, welches kompatibel zum COSO-Ansatz eine konzeptionelle Vertiefung der Anforderungen an eine angemessene Informationsverarbeitung darstellt. *Control Objectives for IT and related Technology* (COBIT) ist ein umfangreiches prozessorientiertes Framework und soll vor allem drei Zielgruppen unterstützen, „das Management für die Abwägung von Risiken und um Kontrolle über Investitionen zu behalten, die Anwender sollen Gewissheit über die Sicherheit und Kontrolle über IT – Dienste haben und die Revisoren bekommen Hilfestellung für interne Kontrollmechanismen und können über das Tool ihre Meinung unterstützen"[38]. Dabei definiert das COBIT Framework detaillierte Kontrollziele und Richtlinien zu kritischen Prozessen und gliedert diese in vier Kategorien: *Plan and Organize,* welche die Qualität zur Überwachung und Korrektur aufgrund der Standards sicherstellen soll und zur Bewertung für mögliche Kor-

[35] Sonnelitter2009, S.1.15 und 1.16.
[36] Vgl. Pickett2010, S.264ff.
[37] COBIT5_2012, S.13.
[38] Helfer2010, S.18.

rekturen der Prozessergebnisse der Kategorien, sowie *Acquire and Implement* und *Deliver and Support*. Die Kategorie *Monitor and Evaluate* rundet den Kreislauf ab und bewertet eine Modifikation der Kategorie Planung und Organisation für den nächsten Kreislauf eines IT-Prozesses. Diese vier Kategorien beschreiben den IT-Produktlebenszyklus, wobei für jede Kategorie Prozesse identifiziert wurden und im COBIT-Modell beschrieben werden. Die Anforderungen aus dem COBIT Framework können zusammengefasst in zwei Kriterien aufgeteilt werden: einerseits sämtliche Ziele, welche einen direkten Einfluss auf die Finanzberichterstattung haben, und andererseits jene Ziele, welche sich nur auf die operativen Aspekte des Unternehmens beziehen.[39]

„*The following summarizes **all** of the information qualities identified in COBIT. (…)*

a. *Primary (direct effect on the reliability of financial reporting):*
    - ***Integrity** relates to the accuracy and completeness of information as well as to whether transactions are valid and authorized.*
    - ***Availability** relates to the information's being available when required by the business now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.*
    - ***Compliance** deals with complying with externally imposed business requirements (…) and relates to the provision of appropriate information for management to exercise its financial and compliance reporting responsibilities.*
b. *Secondary information qualities (no direct impact on financial reporting):*
    - ***Effectiveness** deals with information's being relevant and pertinent to the business processes as well as being delivered in a timely, correct, consistent, and usable manner.*
    - ***Efficiency** concerns the provision of information through the optimal use of resources.*
    - ***Confidentiality** concerns the protection of sensitive information from unauthorized disclosure.*"[40]

[39] Vgl. im Folgenden IIA2008, S.41; Lück2006, S.50; Helfer2010, S.20 und Ramos2006, S.59.
[40] Ramos2006, S.59.

2.3.4 International Organization for Standardization

„International Standards bring technological, economic and societal benefits. They help to harmonize technical specifications of products and services making industry more efficient and breaking down barriers to international trade. Conformity to International Standards helps reassure consumers that products are safe, efficient and good for the environment.“[41]

Die *International Organization for Standardization* (ISO) wurde in London im Jahr 1946 von 65 Delegierten aus 25 verschiedenen Ländern ins Leben gerufen, um eine internationale Standardisierung zu erwirken. Bis heute umfasst ISO rund 19.000 verschiedene Standards, unter anderem den ISO 26000 zur sozialen Verantwortung von Unternehmen, ISO 14001 zur Ermittlung, Kontrolle und Verbesserung der Umweltbelastung eines Unternehmens und ISO 9000, welcher sich mit verschiedenen Aspekten des Qualitätsmanagements befasst.[42]

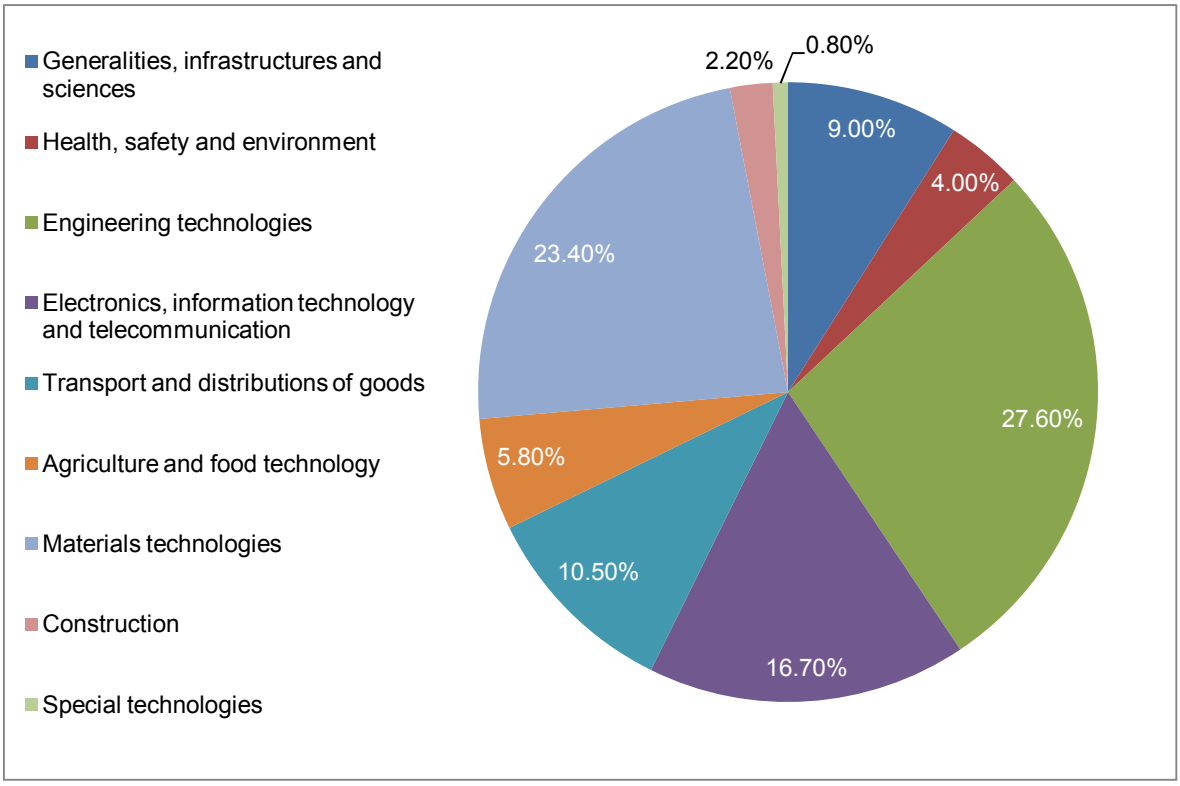

Abb. 2 Aufgliederung der ISO Standards im Jahr 2011[43]

[41] iso.org/Benefits Of ISO Standard, 1. Absatz.
[42] Vgl. im Folgenden iso.org/The ISO Story und iso.org/About ISO, #0, #12, #14, #20 und #21.
[43] Vgl. iso.org/The ISO Story, Grafik #21: „ISO Today“.

In Bezug auf Internal Control gibt es keinen ISO-Standard, der mit dem COSO Internal-Control-Modell zu vergleichen ist, jedoch gibt es vor allem in den ISO 9000 Standards einige Anforderungen, die vor allem die Komponenten des COSO-Modells, *Control Environment*, *Risk Assessment*, *Control Activities*, *Information and Communication* und *Monitoring Activities* stützen. Sowohl die ISO 9000 Standards als auch das COSO Internal-Control-Modell stellen hohe Anforderungen an die Dokumentation von Unternehmensprozessen und die Dokumentation von regelmäßigen Überprüfungen von Systemen und Prozessen, nicht nur in einem einmaligen Verfahren, sondern als kontinuierlicher Prozess, um vor allem die Einführung von Korrekturmaßnahmen sicherzustellen. Ein wesentlicher Unterschied ist jedoch, dass ein Unternehmen unter ISO bestimmte interne Steuerungsprozesse zur Verfügung haben sollte und eine genaue Angabe über die zu testenden Dokumente für einen Prozess enthalten sind, welche von externen Prüfern auf Wirksamkeit bewertet werden müssen und damit sichergestellt sind. COSO hingegen skizziert nur allgemeine Anforderungen, wie der Bedarf an Risikobewertungsverfahren zu decken ist, enthält jedoch keine spezifische Anforderung, wie die Einhaltung der Internal Control zu erreichen ist.[44]

[44] Vgl. im Folgenden Moeller2014, Chapter 17 (e-book) und Stimson2006, S.62.

3 Internal Control als Teil der internen Kontrollorgane

In der heutigen Zeit ist es nicht ungewöhnlich, dass diverse Unternehmenseinheiten zusammenarbeiten, um die Organisation effizienter zu machen und das vorhandene Risiko in allen Unternehmensbereichen zu minimieren. Dabei haben vor allem die Interne Revision, Compliance, Controller sowie Internal-Control- und Risikomanagement-Spezialisten eine spezifische Perspektive und spezifische Kompetenzen im Unternehmen, welche von unschätzbarem Wert für jede Organisation sein können. Jede der Aufgaben trägt einen Teil zur Corporate Governance bei und steht auch in einem engen Zusammenhang mit Internal Control, daher müssen zunehmend Aufgaben koordiniert werden, um sicherzustellen, dass der Internal-Control-Prozess wie vorgesehen funktioniert. Somit müssen klare Verantwortlichkeiten und auch die Grenzen der einzelnen Aufgaben klar definiert werden, um effektiv und effizient alle Lücken in der Kontrolllandschaft zu schließen und eine Doppelberichterstattung zu verhindern.[45]

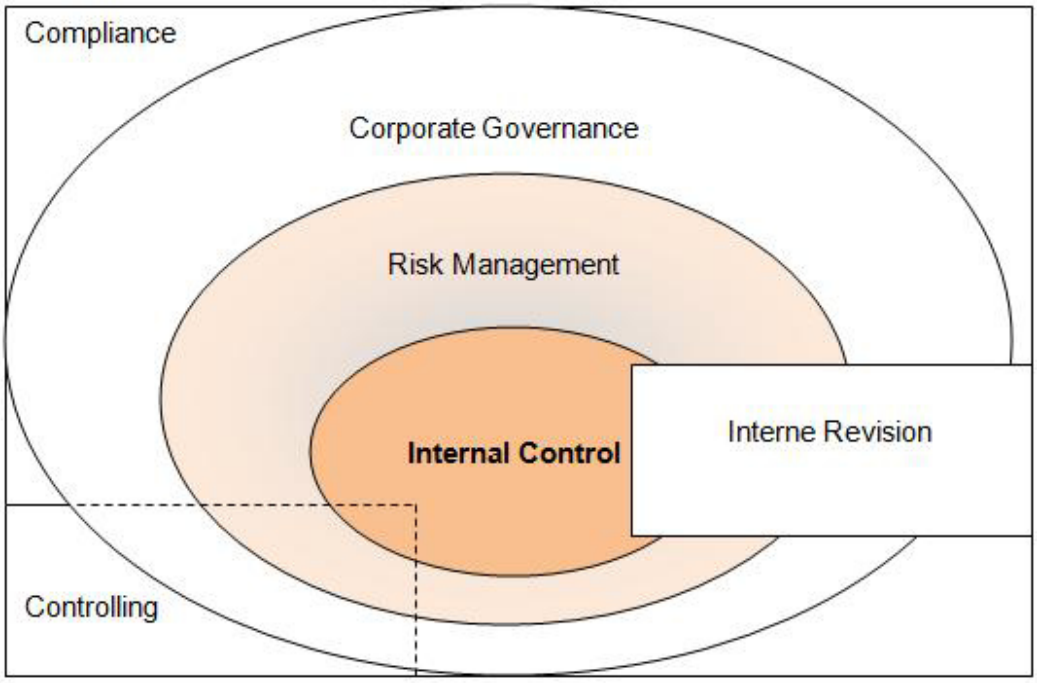

Abb. 3 Internal Control als Teil der internen Kontrollorgane[46]

[45] Vgl. im Folgenden IIA2013/The Three Lines of Defense, S.1f.; Lück2006, S.38; und IIA2004, S.19f.
[46] Vgl. im Folgenden IIA2004, S.19 und Brünger2009, S.19.

3.1 Abgrenzung zu Corporate Governance

3.1.1 Definition Corporate Governance

„*Corporate governance is the system by which business corporations are directed and controlled. Boards of directors are responsible for the governance of their companies. The shareholders' role in governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place. The responsibilities of the board include setting the company's strategic aims, providing the leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship. The board's actions are subject to law, regulations and the shareholders in general meeting.*"[47]

Diese Definition von Corporate Governance aus dem Jahr 1992 vom *Committee on the Financial Aspects of Corporate Governance*, zusammengesetzt von der Londoner Börsenaufsicht, mit über 200 Mitgliedern, welche achtzehn Monate für die Erstellung des *Report of the Committee on the Financial Aspects of Corporate Governance* gebraucht hat, führte zu einem Umdenken hin zu den Grundsätzen der Offenheit, Integrität und Rechenschaftspflicht als dem Wesen der Unternehmensführung in vielen anderen Ländern. Corporate Governance umfasst dabei viele verbindliche und freiwillige Maßnahmen, wie die Einhaltung von Gesetzen und Regelwerken, das Befolgen von anerkannten Empfehlungen und das Einführen und Einhalten von unternehmensinternen Leitfäden. Um Corporate Governance in einem Unternehmen sicherzustellen, muss die Implementierung von Strukturen zur Leitung und Kontrolle eines Unternehmens festgelegt sein. Dazu müssen Strategien und Ziele festgelegt und Maßnahmen gesetzt werden, die zur Zielerreichung und der Umsetzung von Strategien beitragen, die Überwachung der Unternehmensleistung sichergestellt sein und dementsprechende Überwachungssysteme implementiert sein. Zusammengefasst enthält Corporate Governance demnach folgende Elemente[48]:

a. „Steuerungs- und Überwachungssystem
    - Strategien
    - Risikofähigkeit
    - Risikomanagementsystem
        - Aufbau- und Ablauforganisation
        - Risikocontrolling
        - Berichtswesen
        - Interne Revision

[47] Ecgi1992/Financial Aspects of Corporate Governance, § 2.5.
[48] Vgl. im Folgenden Clarke2012, S.1ff.; Bloomfield2013, S.7ff.; Helfer2010, S. 70 und Steckel2007, S.20.

b. Organe / Interessengruppen
    - Aufsichtsorgan
        - Prüfungsausschuss
    - Vorstand
    - Interne Funktionsbereiche
    - Sonstige (Abschlussprüfer, Träger, Eigentümer, Aufsicht, Öffentlichkeit)
c. Rechtliche Rahmenbedingungen (…)
d. Unternehmensgrundsätze
    - Geschäftsanweisung für das Aufsichtsorgan
    - Geschäftsanweisung für den Vorstand
    - Strategien
    - Geschäftsanweisung für die Interne Revision
    - Kommunikationsregeln
    - Organisationsrichtlinien
    - Unternehmensleitbild
    - Führungsgrundsätze
    - Ziel- und Vergütungssysteme“[49]

3.1.2 Internal Control als Teil der Corporate Governance

Als Ergebnis eines Umdenkens in den letzten Jahren, dem zufolge das Interesse der institutionellen Investoren zusehends in den Vordergrund gerückt ist, kann Corporate Governance als ein fairer und transparenter Mechanismus verstanden werden, um langfristigen Unternehmenswert zu schaffen und um den Nutzen für die gesamte Gesellschaft zu steigern. Vor allem wurden eine Vielzahl von Regelungen geschaffen und weitestgehend regulatorische und legislative Änderungen durchgesetzt, um den Investoren mit besseren Governance-Praktiken und -Leitlinien zur Unternehmensführung mehr Sicherheit für ihre Investitionen zu geben und um der Unternehmensleitung die Festlegung von Strategien zu erleichtern, welche die Wertschöpfung fördern. Einen zentralen Einfluss auf die Corporate Governance hat in diesem Kontext vor allem der *Sarbanes-Oxley Act*, welcher in den USA „mit der Zielsetzung, die Corporate-Governance-Anforderungen besonders hinsichtlich interner Kontrollen, Dokumentation und erweiterter Offenlegungspflichten für Unternehmen zu ergänzen“[50], veröffentlicht wurde und vor allem den Schutz der Anleger als wichtigstes Ziel definiert. Corporate Governance soll demnach interne Instrumente anbieten, um potenzielle Risiken und Informationen mit negativem Einfluss darzustellen, und damit ein Abbild der Wirklichkeit uneingeschränkt richtig und vollständig aufzeigen. Mit dieser Veränderung der Publizitätspflichten wurde auch ein internes Kontrollsystem

[49] Helfer2010, S.71.
[50] Welge2012, S.45.

zur Erkennung, Dokumentation und Verhinderung potentieller Fehlerquellen in der Finanzberichterstattung eingefordert und damit eine neu geforderte Transparenz, Kontrolle und Integrität für die Investoren und Anleger garantiert. „Demgemäß wird Corporate Governance als eine verantwortliche und auf langfristige Wertschöpfung zielende Unternehmensführung sowie Unternehmenskontrolle verstanden“[51], wobei Unternehmenskontrolle nach SOX vom externen Abschlussprüfer und vom Management auf Fehler und Störungen überprüft werden muss, um eine Vergleichbarkeit sicherzustellen, und nach einem einheitlichen und anerkannten Rahmenwerk festgelegt sein muss. Das COSO Internal Control Framework wurde hier als Referenzmodell festgelegt.[52]

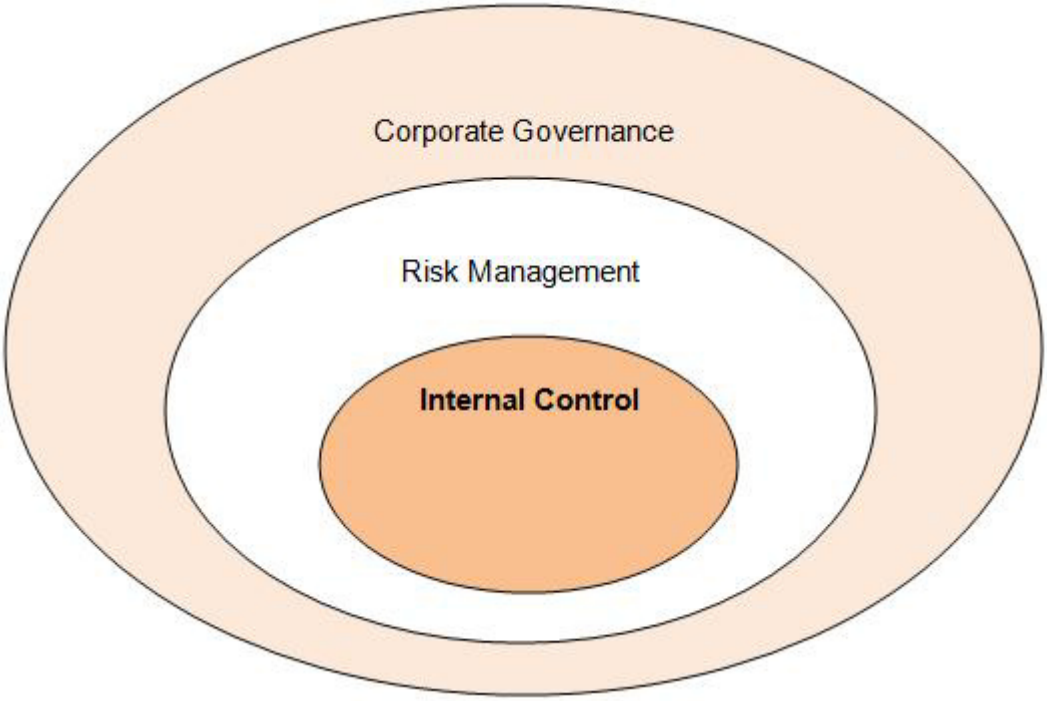

Abb. 4 Internal Control als Teil von Corporate Governance[53]

Das COSO-Rahmenwerk definiert Internal Control als einen Prozess, „der von Management, Gremien und Mitarbeitern ausgeübt wird, um festgelegte Ziele mit ausreichender Sicherheit zu gewährleisten“[54] und ist in fünf Hauptkomponenten aufgeteilt, welche man im COSO-Rahmenwerk für Enterprise Risk Management wiederfindet. Das COSO-ERM stellt eine Weiterentwicklung des COSO IC dar und wird damit ein integrierter Bestandteil

[51] Knapp2005, S.59.
[52] Vgl. im Folgenden A.C.2009, S.76; Brünger2009, S.18f.; Root1998, S.10f.; Welge2012, S.45ff. und Knapp2005, S.59.
[53] Vgl. Brünger2009, S.19.
[54] Welge2012, S.48.

des Enterprise Risk Management und zeigt Internal Control als Bestandteil des unternehmensweiten Risikomanagementsystems. Beide Komponenten, sowohl Internal Control als auch Enterprise Risk Management, müssen nach COSO in allen Organisationseinheiten implementiert werden und zeigen nur in den einzelnen Ausprägungen Unterschiede auf. Damit werden beide Aspekte als wichtiger Teil für eine gut funktionierende Corporate Governance gesehen.[55]

[55] Vgl. im Folgenden Brünger2009, S.18f. und Welge2012, S.47ff.

3.2 Abgrenzung zur Internen Revision

3.2.1 Definition Interne Revision

Als Interne Revision wird eine im eigenen Unternehmen angesiedelte, unabhängige und objektive Prüfungs- und Beratungsstelle bezeichnet, die eine Organisation bei der Umsetzung der Ziele durch systematische und objektive Bewertung und Verbesserung der Effektivität des Risikomanagements, der Kontrollen und des Governance-Prozesses unterstützt. Die Interne Revision hat dabei die Prüfungsausrichtung der Ordnungsmäßigkeit, Wirtschaftlichkeit und Sicherheit und ist Teil der Organisation, deren Ziele von internationalen Standards, dem Vorstand und vom Management vorgegeben werden. Sie befasst sich mit monetären und nichtmonetären Aspekten der Organisation und schafft einen Mehrwert durch eine kontinuierliche Überprüfung und Bewertung der Prozesse und Kontrollen. Dabei soll die Unternehmensleitung bei den Überwachungs- und Steueragenden unterstützt, Schwachstellen identifiziert und aufgezeigt und Verbesserungen beauftragt werden, was nur erfolgen kann, wenn die Risikofaktoren des Unternehmens bekannt sind, Anpassungen initiiert und Maßnahmen zur Reduzierung von Risiken eingeleitet werden. Weiter wird durch die Interne Revisionseinheit eine Prüfung und Beurteilung des Internen Kontrollsystems durchgeführt, und auch das Thema Anti Fraud Audit wird durch die zunehmende Bedeutung abgedeckt. Im Vergleich dazu wird die Externe Revision primär durch Statuten geleitet und vom Vorstand bestellt, um eine unabhängige Meinung über die Finanzberichterstattung des Unternehmens bereitzustellen und darzulegen, ob die Darstellung des Jahresabschluss den anerkannten Grundsätzen der Rechnungslegung entsprechen und damit die finanzielle Lage des Unternehmens für die angegebene Periode richtig und wesentlich dargestellt wurde.[56]

Eine der anerkanntesten Leitlinien für die Interne Revision bietet *The Institute of Internal Auditors* (IIA), welche durch Veröffentlichung des *International Professional Practices Framework* (IPPF), eine offizielle Definition und eine Reihe von internationalen Standards für die berufliche Praxis der Internen Revision, sowie den *Code of Ethics* (der über die grundsätzliche Definition der Internen Revision hinausgeht, durch die Beschreibung von Grundsätzen, die den Berufsstand und die Prüfungspraxis der Internen Revision betreffen und Regeln, die beschreiben wie sich Interne Revisoren verhalten sollen, um die Grundsätze in die Praxis umzusetzen, und dabei einen Wegweiser für ethisches Verhalten darstellt) zur Verfügung stellt und damit eine Mindestanforderung für alle *Certified Internal Auditors* (CIA) aufstellt. Die Prüfung zum CIA wird weltweit einheitlich angeboten, umfasst eine einheitliche Aufgabenstellung und ein einheitliches Anforderungsprofil, zählt zu ei-

[56] Vgl. im Folgenden Füss2005, S.34f.; IIA2014/Frequently Ask Questions und IIA2008, S.21.

nem der umfassendsten Zertifikate für einen Internen Revisor und bietet einen Nachweis über alle Bereiche der Internen Revision[57]

3.2.2 Internal Control als Teil der Internen Revision

Für ein Unternehmen besteht immer die Gefahr, dass ein Ereignis, eine Handlung oder das Unterlassen einer Handlung die Fähigkeit eines Unternehmens, seine Ziele zu erreichen oder gemäß der Unternehmensstrategie zu handeln, negativ beeinflusst. Um sich vor solchen Risiken abzusichern, stützen sich Unternehmen auf *The Three Lines of Defense* Modell, welches eine Möglichkeit bietet, in den drei wichtigsten Corporate-Governance-Teilen wesentliche Aufgaben und Pflichten zu klären und damit die Wirksamkeit der jeweiligen Instrumente zu verbessern. An erster und zweiter Stelle stehen die prozessabhängigen Kontrollfunktionen, also das Interne Kontrollsystem, das aus Regelungen zur Steuerung der Unternehmensaktivtäten und zur Überwachung der Einhaltung dieser Regelungen besteht, und das Risikomanagement, also Risikopolitik, Früherkennungssystem und operatives Risikomanagement. An dritter Stelle steht die prozessunabhängige Interne Revision, die innerhalb eines Unternehmens Strukturen und Aktivitäten prüft und beurteilt und damit auch die Prüfung aller prozessbezogenen Kontrollen durchführt. Ein wesentlicher Aufgabenbereich der Internen Revision ist also die Prüfung des Internen Kontrollsystems und Risikomanagements. Dabei kann eine Prüfung der Internen Revision über das interne Kontrollsystem in verschiedenen Formen wahrgenommen werden: ein Soll-Ist Vergleich soll sicherstellen, ob das in den Prozessen implementierte Interne Kontrollsystem mit dem geplanten übereinstimmt, eine Überprüfung der implementierten Internen Kontrollmaßnahmen auf ihre Effizienz und Wirksamkeit sowie die richtige Durchführung der Kontrollen von den verantwortlichen Mitarbeitern und die Sicherstellung, dass der geplante Kontrollprozess noch mit der aktuellen Prozesslandschaft übereinstimmt. Eine wesentliche Aufgabe der Internen Revision in Bezug auf das Interne Kontrollsystem ist neben der Prüftätigkeit auch eine beratende Funktion. Da in der Regel die Interne Revision einen gesamten Überblick über die unternehmensweiten Prozesse hat, kann eine aktive, risikopräventive Beratung und auch Projektbeteiligung angeboten werden, welche als Grundlage für die Gestaltung von Internen Kontrollen herangezogen werden kann.[58]

Diese Anforderungen an die Interne Revision mit der Überprüfung des Internen Kontrollsystems wird vor allem mit der Verabschiedung des SOX deutlich, da dieser eine zentrale Komponente zur Implementierung und Aufrechterhaltung eines Internen Kontrollsystems

---

[57] Vgl. im Folgenden IIA2013/Standards-Guidance, S.6f. sowie S.15; IIA2014/Frequently Ask Questions und IIA2008, S.76.

[58] Vgl. im Folgenden IIA2004, S.21ff.; Sommer2010, S.24f.; Burger2012, S.84f.; Freidank2008, S.28; Lück2009, S.165ff.; Steckel2007, S.17ff. und IIA2013/The Three Lines of Defense, S.2ff.

definiert und eine jährliche Wirksamkeitsbeurteilung und Einschätzung des Managements über die Effektivität des einzurichtenden Kontrollsystems, speziell in Bezug auf die Finanzberichterstattung, fordert. Die Sec. 404 SOX präzisiert die Anforderung „wonach der externe Abschlussprüfer die Effektivität des Internen Überwachungssystems in Bezug auf die Finanzberichterstattung zu prüfen hat, (…) hierzu gehört auch die systematische Aufnahme und Analyse der Geschäftsprozesse.“[59] Des Weiteren wird in der Sec. 302 SOX gefordert, dass eine Bestätigung vom Vorstandsvorsitzenden und des Finanzvorstands über das Internal Control gegeben wird, wobei man hier die Subzertifizierung in der Verantwortung der Internen Revision sehen kann indem das Management unterhalb des Vorstands die Verantwortung übernimmt und dem Vorstand vorab die relevante Bestätigung liefert.[60]

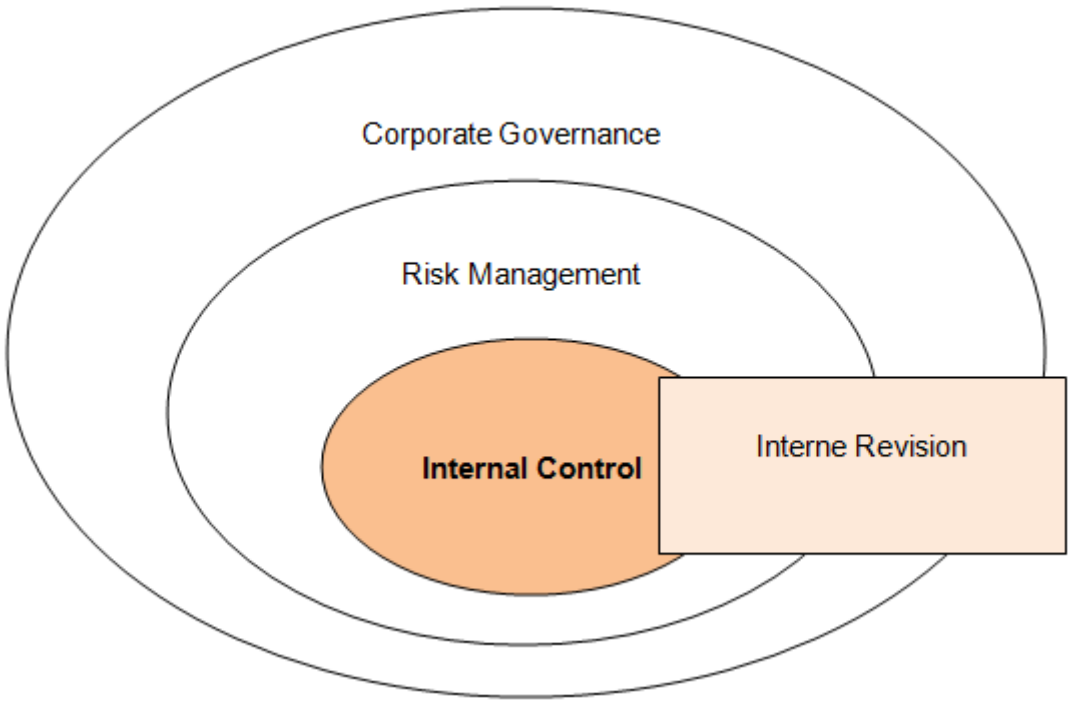

Abb. 5 Interne Revision als Teil der Internen Kontrollorgane[61]

[59] Freidank2008, S.36.
[60] Vgl. im Folgenden Freidank2008, S.36f. und IIA2004, S.17.
[61] Vgl. im Folgenden IIA2004, S.19 und Brünger2009, S.19.

3.3 Abgrenzung zu Compliance

3.3.1 Definition Compliance

Viele Unternehmen haben verschiedene finanzielle, betriebliche, operative und rechtliche Risiken falsch eingeschätzt, und es wurde ein erheblicher Mangel in den Risikomanagementsystemen aufgezeigt. Dadurch hat der Begriff Compliance, welcher ursprünglich von *to comply with* abgeleitet wird und „die Erfüllung bzw. Konformität mit staatlichen Restriktionen, Regeln und Spezifikationen sowie mit ethischen und moralischen Grundsätzen, aber auch mit Standards und Richtlinien“[62] umschreibt, einen neuen Stellenwert bekommen. Compliance kann dabei mit Corporate Governance verglichen werden, obwohl ein wesentlicher Unterschied in der Betrachtungsperspektive auf die Standards für Unternehmensführung und -kontrolle besteht, da „Compliance den Blickwinkel der ‚Regulierten‘, also der betroffenen Unternehmen, umschreibt, und Corporate-Governance-Grundsätze der Verwirklichung einer verantwortlichen, auf Wertschöpfung ausgerichteten Leitung und Kontrolle von Unternehmen und Konzernen dienen..[63] Compliance unterstützt das Unternehmen, indem es dazu beiträgt, dass finanzielle Risiken und Haftungsrisiken reduziert, Wettbewerbsvorteile geschaffen werden, das Vertrauen von Stakeholder gestärkt und das Ansehen in der Öffentlichkeit für ein Unternehmen verbessert wird.[64]

Ziel von Compliance ist die Einhaltung gesetzlicher Normen oder unternehmensspezifischen Vorgaben, um rechtliche Nachteile sowie Reputationsschäden für das Unternehmen und deren Mitarbeiter zu vermeiden. Um Compliance-Vorgaben in einem Unternehmen umzusetzen, muss ein Compliance-Konzept erstellt und vom Management kommuniziert und vorgelebt werden (*tone at the top*), um diese Vorgaben dann in der Regel von einer Compliance-Organisation durchsetzen zu lassen. Ein funktionierendes Compliance-System steigert die Wettbewerbsfähigkeit durch eine Präventivwirkung, die die Nachhaltigkeit des wirtschaftlichen Erfolges durch ein gezieltes Risikomanagement von vorsätzlich durchgeführten Handlungen zum Schaden des Unternehmens, wie zum Beispiel Bilanzmanipulation, Untreue oder Unterschlagung, fördert.[65]

[62] Petsche2012, S.1.
[63] Petsche2012, S.6.
[64] Vgl. im Folgenden Petsche2012, S.1ff. und IIA2006, S.32f.
[65] Vgl. im Folgenden Petsche2012, S.47f. und CFOaktuell2013_96, S.97f.

3.3.2 Internal Control als Teil von Compliance

Die Kontrollfunktion im Unternehmen soll sicherstellen, dass alle Vorgaben im Unternehmen eingehalten werden, dazu zählen auch Compliance-relevante Richtlinien, Regeln und Gesetze, wie zum Beispiel die Kontrolle von Interessenskonflikten oder Insiderinformationen bzw. ob eine Tätigkeit einschlägigen Normen entspricht. Diese Compliance-Prozesse müssen einer regelmäßigen und dauerhaften Überwachung unterzogen werden, sind damit Teil von prozessbegleitenden Überwachungsmaßnahmen; und somit ist Compliance ein Teil des Internen Kontrollsystems. Eine der Voraussetzung für Internal Control ist die Setzung von Zielen, die auf operative Tätigkeiten und die dadurch entstehenden Bedürfnisse des Unternehmens ausgerichtet sind, damit Wertschöpfung für alle Stakeholder geschaffen oder bewahrt wird und diese sich nach Gesetzen, Regeln, Vorschriften und Normen durch den Gesetzgeber oder internen Richtlinien richten. Das COSO Framework unterteilt diese Ziele in drei Kategorien, *Operations, Reporting* und *Compliance*, wobei Compliance die Verantwortung einer Einheit darstellt „*to conduct activities, and often take specific actions, in accordance with applicable laws and regulations. As part of specifying compliance objectives, the organization needs to understand which laws, rules and regulations apply across the entity. (…) For purpose of the COSO Framework, compliance with an entity's internal policies and procedures, as opposed to compliance with external laws and regulations (…), relates to operations objectives*."[66] Um die Einhaltung der Anforderungen des Internen Kontrollsystems in Bezug auf Compliance sicherzustellen, müssen wesentliche Prozesse geschaffen werden und bereits bestehende Prozesse auf die Förderung von regelkonformen Verhalten überprüft werden, da die meisten Compliance-Verfahren selbst verwaltet sind, direkt in der Verantwortung des Managements liegen und die Compliance Informationen in die relevanten Berichte einfließen. Dies erfordert ein hohes Informations- und Bildungsniveau in allen Einheiten, sodass alle Interessengruppen über die Einhaltung dieser Anforderungen informiert sind, um die wesentlichen Internen Kontrollen abzudecken. Es sollte des Weiteren eine regelmäßige Überprüfung des Internen Kontrollsystems auf die Abdeckung von spezifischen Compliance Risiken stattfinden.[67]

Fraud ist „eine beabsichtigte Falschdarstellung der Wahrheit, um jemanden im Vertrauen darauf zur Aufgabe eines Vermögensgegenstands oder eines seiner Rechte zu veranlassen. Eine falsche Darstellung von Fakten in Form von Worten oder Taten durch irreführende Behauptungen oder durch Verschleierung von notwendigen Angaben, sodass jemand aufgrund dieser Täuschung aus seinem rechtlichen Nachteil handelt"[68], und die Verhinderung oder Aufdeckung von solchen Betrugshandlungen sind primär der Compliance zugeordnet, haben aber vor allem im neuen COSO Internal Control Framework als einem der Kernprinzipen („*Principle 8: The organization considers the potential for fraud in*

[66] COSO2013, S.9 und S.10.
[67] Vgl. im Folgenden COSO2013, S.6ff.; Petsche2012, S.74f. sowie S.90f. und Moeller2014, Chapter 11 (e-book).
[68] Petsche2012, S.448.

assessing risks to the achievement of objectives“[69]) für Internal Control einen hohen Stellenwert. Dabei werden vier Eigenschaften, *considering various types of Fraud, assessing incentive and pressures, assessing opportunities* und *assessing attitudes and rationalizations*, im Zusammenhang mit Fraud beschrieben, um eine ausreichende Kontrolllandschaft zu formulieren, die bei der Verhinderung von Betrug im Allgemeinen unterstützen soll und damit der Zielkategorie Compliance zuzuordnen ist. Vor allem die als erster Schritt beschriebene Erkennung der Arten von Fraud sind Deckungsgleich mit dem *Fraud Tree*, welcher von der *Association of Certified Fraud Examiners* (ACFE) im Jahr 1996 erstmals veröffentlicht wurde und eine Darstellung von Delikten und deren Ausprägungen darstellt, Korruption, Absicherung von Vermögen und Manipulation der Finanzberichterstattung.[70]

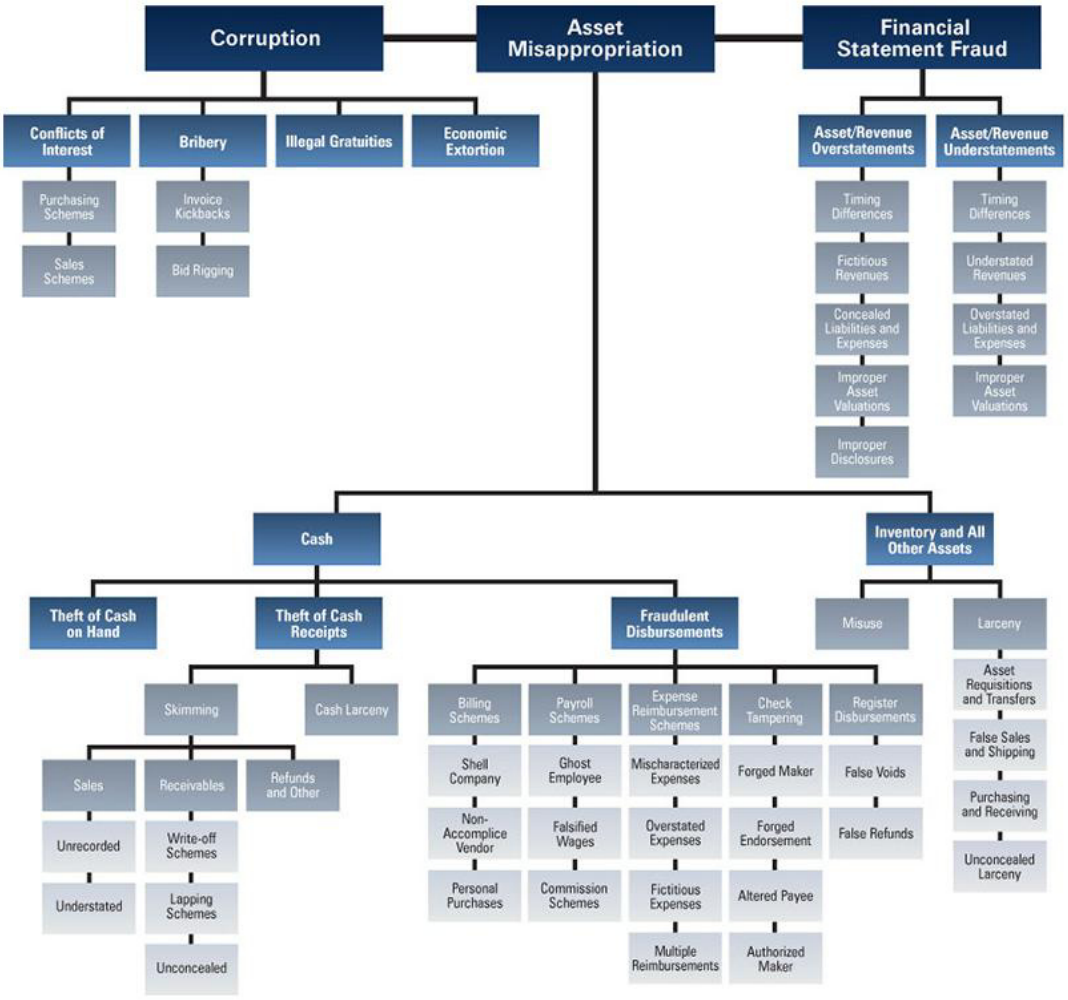

Abb. 6 Fraud Tree der Association of Certified Fraud Examiners[71]

[69] COSO2013, S.78.
[70] Vgl. im Folgenden COSO2013, S.78ff. und Petsche2012, S. 451ff. sowie S.459.
[71] ACFE2014/Fraud Tree

Im Rahmen des Assessments selbst sollten dann alle Geschäftsprozesse mit einer Fraud Relevanz identifiziert werden und die Kontrollmechanismen und -maßnahmen definiert bzw. angepasst werden, vor allem da Fraud einen Einfluss auf das gesamte Unternehmen und dessen Kontrollumfeld haben kann.[72]

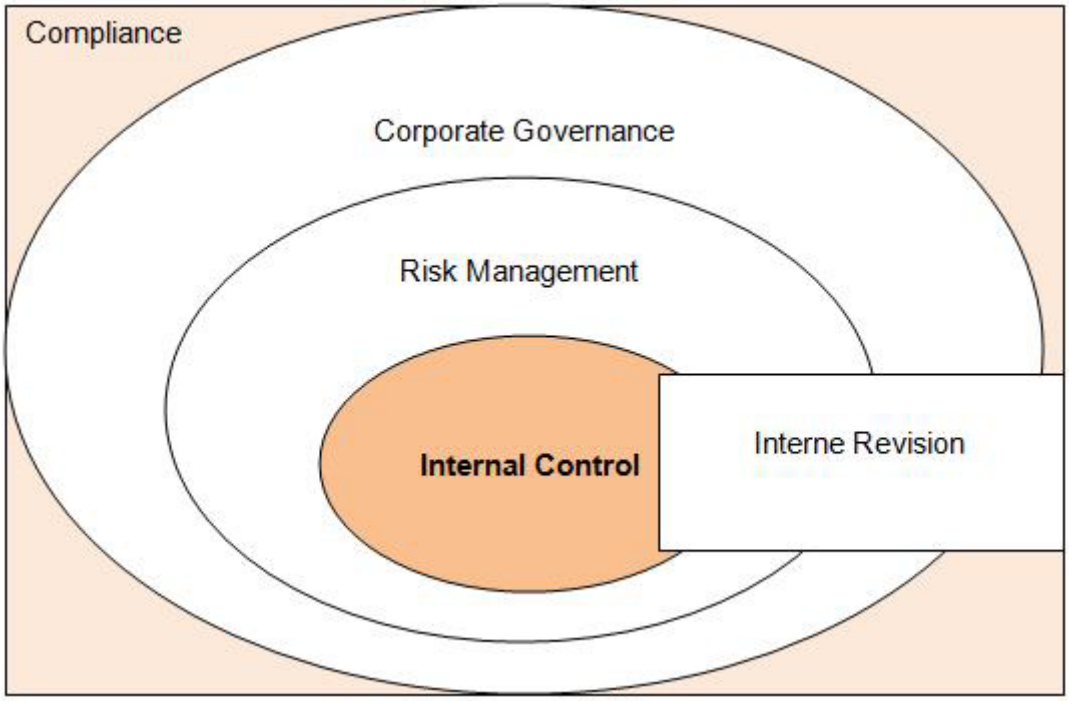

Abb. 7 Compliance als Teil der Internen Kontrollorgane[73]

[72] Vgl. im Folgenden COSO2013, S.78ff. und Petsche2012, S. 451ff. sowie S.459.
[73] Vgl. im Folgenden IIA2004, S.19 und Brünger2009, S.19.

3.4 Abgrenzung zu Controlling

3.4.1 Definition Controlling

Grundsätzlich darf man Controlling nicht mit „*Control*“, also auf Deutsch „Kontrolle“, übersetzen, da die sinngemäße Übersetzung im Sinne von Controlling, also die Steuerung, als zentrale Managementaufgabe zu verstehen ist. Die Zielsetzung des Controllings umfasst dabei die zielgerichtete Koordination von bestehenden Prozessen als Steuerungshilfe bei der Planung, Informationsversorgung, Kontrolle und Steuerung mit den im Unternehmen vorhandenen Planungsdaten, welche den Unternehmenszielen entsprechen, im Zeitraum des noch laufenden zu kontrollierenden Prozesses oder unmittelbar nach Abschluss eines Prozesses. Dabei ist Controlling ein prozessabhängiges Führungssystem, also ein Instrument, um zu einer praktischen Erreichung von vereinbarten Unternehmenszielen zu führen. Eine Organisation und die Überwachungshandlung selbst sind dabei immer zukunfts- und ergebnisorientiert, jedoch durch die häufige Zusammenarbeit mit den betroffenen Organisationsteilen als eine abhängige Prüfungsinstitution zu sehen. Als „Erweiterung des betrieblichen Rechnungswesens, das ursprünglich durch vergangenheitsorientierte Rechnungssysteme wie die Buchhaltung und Istkostenrechnung geprägt war, soll im Hinblick auf planerische, kontrollierende und informationelle Prozesse ein Beitrag zur zukunftsorientierten Unternehmensführung geleistet werden.“[74] Aus dieser Grundfunktion des Controllings können vier Konzeptionen für ein Unternehmen entwickelt werden[75]:

- „Die gewinnzielorientierte Konzeption hat zum Inhalt, dass das Controlling seine Maßnahmen am Gewinnziel des Gesamtunternehmens auszurichten hat.
- Die informationsorientierte Auffassung sieht das Controlling als Unterstützungsfunktion, indem durch die Versorgung mit Informationen Managemententscheidungen vorbereitet werden.
- Mit der koordinationsorientierten Controlling – Konzeption wird auf die Abstimmung einzelner Teilbereiche im Führungssystem (u.a. Planungs-, Kontroll-, Personalführungssystem) abgestellt.
- (…) Die planungs- und kontrollorientierte Konzeption stellt die Notwendigkeit der Abstimmung von Planung und Kontrolle in den Fokus der Betrachtung. Schwerpunkt des Controllings bildet dabei die Unternehmensplanung, insbesondere die Planungs- Entscheidungsfindungs- und Kontrollrechnungen.“[76]

[74] Stelling2005, S.10.
[75] Vgl. im Folgenden Horvath2012, S.17; Horvath2003, S.319; Stelling2005, S.10f. und Füss2005, S.60f.
[76] Füss2005, S.60.

3.4.2 Internal Control als Teil des Controllings

Von der Ableitung des Begriffes Internal Control zu Controlling kann ein Zusammenhang angenommen werden, welcher sich vor allem in zwei Gemeinsamkeiten widerspiegelt. Sowohl Internal Control als auch Controlling verwenden einen Soll-Ist Vergleich als Grundlage für die Umsetzung von Unternehmenszielen, welches die zweite Gemeinsamkeit darstellt. Beide bezwecken in erster Linie die Erreichung der Unternehmensziele zu unterstützen, unterscheiden sich jedoch trotz der kontinuierlichen Umsetzung in der Art und Weise des Vorgehens und der Zielsetzung. Internal Control wird als Konzept, Prozess und System ausgestaltet, für das die Mitarbeiter eines Unternehmens, je nach Grad der jeweiligen Verantwortung, zuständig sind. Das Controlling stellt eine eigene Funktion in einem Unternehmen dar, und der Controller hat die Zuständigkeit dafür inne. Im Rechnungswesen eines Unternehmens hat das Controlling die stärksten Berührungspunkte mit dem Internen Kontrollsystem, da es wesentlich zur Definition der internen Kontrollen, besonders betreffend die Sicherheit und Zuverlässigkeit der Informationen, beiträgt. Controlling stellt eine Steuerungshilfe für das Management in der Planung, Kontrolle und Informationsversorgung dar und leistet damit einen wichtigen Beitrag für die Ergebnis-, Finanz-, Prozess- und Strategietransparenz und soll das Unternehmen in Richtung der Einhaltung und Umsetzung der Rentabilitäts-, Liquiditäts- und Wirtschaftlichkeitsziele steuern. Auf der anderen Seite gewährleistet Internal Control die prozessabhängige Interne Steuerung und Kontrolle sowie die prozessunabhängige Prüfung und stellt dabei sicher, dass Tätigkeiten wirksam und effizient funktionieren, die interne und externe Berichterstattung verlässlich ist und dass Gesetze und Normen eingehalten werden.[77]

Controller nehmen auch Kontrollaufgaben wahr, aber eben mehr im Sinne von prozessbegleitender Steuerung und nicht zur unabhängigen Kontrolle, sondern durch Soll-Ist Vergleiche zur Planung und für die Sicherstellung von Genehmigungsvorgängen. „In Bezug auf den konkreten Durchlauf der Internal-Control-Instrumente kann das Controlling einerseits eine Prozessverantwortung übertragen erhalten und andererseits die Einhaltung der geltenden Normen kontrollieren. Schließlich gilt es, Kontrollergebnisse zu ermitteln, Abweichungen festzustellen, diese zu analysieren und in Reports an das Management zu dokumentieren.“[78] [79]

[77] Vgl. im Folgenden Jenal2012, S.7f. und IIA2004, S.24f.
[78] Burger2012, S.125.
[79] Vgl. im Folgenden Burger2012, S.124f. und Maier2006, S.42f.

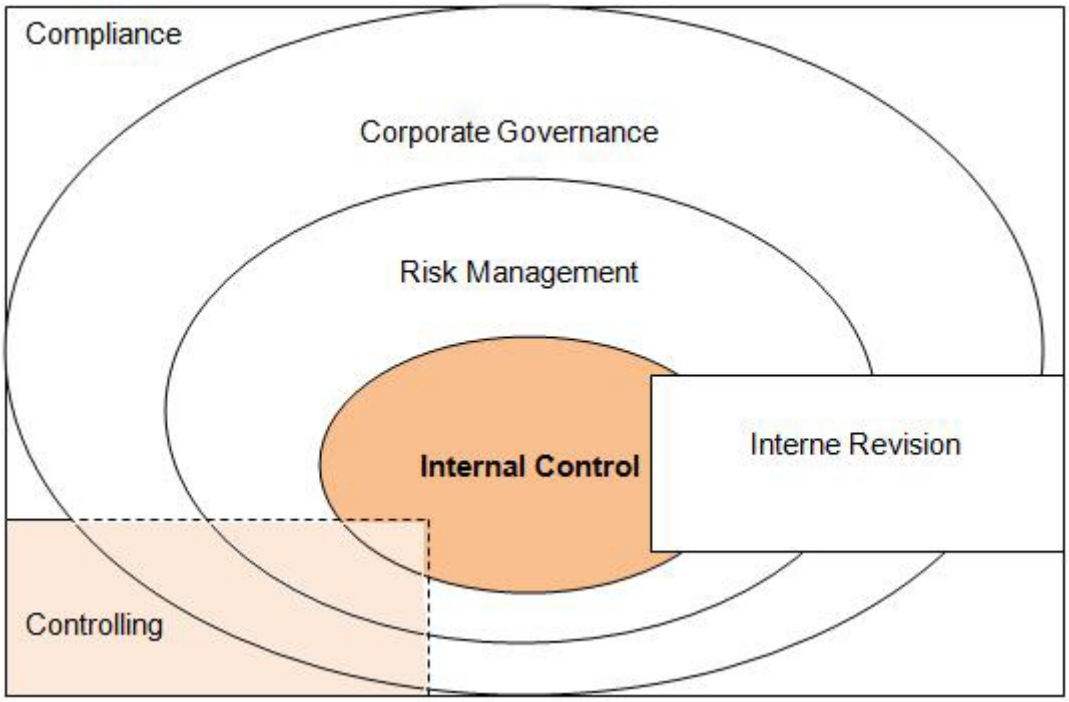

Abb. 8 Controlling als Teil der internen Kontrollorgane[80]

[80] Vgl. im Folgenden IIA2004, S.19 und Brünger2009, S.19.

4 Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework

Aufgrund von verschiedenen Unternehmensskandalen in den Vereinigten Staaten von Amerika Anfang der 90er Jahre wurde von den Sponsoring Organizations, American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives Institute (FEI), Institute of Internal Auditors (IIA) und Institute of Management Accountants (IMA) das Committee of Sponsoring Organizations of the Treadway Commission gegründet. Dieser Ausschuss setzte sich aus 6 Kommissionsmitgliedern, über 20 Mitarbeitern, einem 12-köpfigen Beirat zusammen und dem Vorsitzenden James C. Treadway jr., daher auch die Bezeichnung “Treadway“ Commission. Ziel dieser Kommission ist es, einheitliche, allgemein anerkannte Standards und Methoden als generelles Internal-Control-Konzept, welches sowohl für Non-Profit- als auch für Profit-Unternehmen Gültigkeit hat, zu konzipieren. Dieses Konzept wurde 1991 mit dem Titel „Internal Control – Integrated Framework veröffentlicht und beinhaltet neben einer Definition von Internal Control als einem vom Management initiierten Prozess, der keine absolute Sicherheit bezüglich der Zielerreichung gewährleisten kann, auch die Ziele und fünf Komponenten des Internal Control, welche in wechselseitiger Verbindung mit der Aufbau- und Ablauforganisation des Unternehmens stehen, und stellt damit ein Regelwerk zur Einrichtung von Internen Kontrollsystemen zur Verfügung. Die Etablierung des COSO Internal Control – Integrated Framework wird mittlerweile sowohl von der Securities and Exchange Commission (SEC) als auch vom Public Company Accounting Oversight Board (PCAOB) nachhaltig empfohlen, und damit gilt dieses als eine wesentliche Regelung und als Benchmark für die Einrichtung und Funktionsfähigkeit von Internen Kontrollsystemen.[81]

[81] Vgl. im Folgenden Helfer2010, S.9f.; IIA2004, S.15f.; IIA2006, S.22 und Lück2006, S.39.

4.1 Committee of Sponsoring Organizations of the Treadway Commission

4.1.1 Entstehung des Committee of Sponsoring Organizations of the Treadway Commission

Die Notwendigkeit von Kontrollen in Unternehmen wurde schon sehr früh erkannt, um ein Unternehmen zu lenken, Aktivitäten zu überwachen und damit die Ziele der Einheit sicherzustellen. Im Laufe der Zeit hat sich, vor allem durch Fälle von Betrug, die Bedeutung des internen Kontrollsystems für den Erfolg eines Unternehmens hervorgehoben. Es gab eine wachsende Entwicklung von effektiven Management-Praktiken zur Orientierungshilfe für Mitarbeiter und die Erstellung von Kontrollen über viele Aktivitäten. Die erste Definition von Internal Control wurde im Jahr 1949 vom *Committee on Auditing Procedure* des *American Institute of Accountants* (*AIA*), das heutige *American Institute of Certified Public Accountants* (*AICPA*), herausgegeben[82]:

„*Internal Control comprises the plan of organization and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, an encourage adherence to prescribed managerial policies.*"[83]

Später wurde die Originaldefinition erweitert, um das Konzept von Verwaltungs- und Rechnungslegungs- Kontrollen einzuschließen. Internal Control als Begriff mit einer Reihe von Berichten, Richtlinien und Normen mit einer Auswirkung auf die interne Kontrolle in der Wirtschaftsprüfung wird jedoch bereits seit den Anfängen des neunzehnten Jahrhunderts behandelt, und seit den siebziger Jahren ist die Prüfung des Internal Control auch als eine der Berufspflichten der Abschlussprüfer durch das von der AICPA herausgegebenen *Statements on Auditing Procedure No.54 - The Auditor's Study and Evaluation of Internal Control* festgelegt. Nach dem Watergate-Skandal in den 1970er Jahren, in dem aufgedeckt wurde, dass von Unternehmen Bestechungsgelder und illegale Parteispenden an Politiker gezahlt worden waren, wurde von der SEC der *Foreign corrupt Practices Act of 1977* (FCPA) in Kraft gesetzt, welcher Anti-Korruptions-Bestimmungen und Bilanzierungs- und Interne Kontrollen enthält. Das Management wird dabei dazu verpflichtet, Aufzeichnungen zu führen und alle Transaktionen genau und wahrheitsgetreu aufzuzeichnen und widerzugeben. Damit soll sichergestellt werden, dass „alle Transaktionen nur mit Wissen und Genehmigung des Managements ausgeführt werden, der Einsatz von Unternehmensvermögen auf die vom Management genehmigten Zwecke beschränkt ist und ein periodischer Vergleich der buchhalterischen Aufzeichnungen mit den tatsächlichen Ver-

82 Vgl. im Folgenden Klawatsch1995, S.5; COSO1994, S.93 und AICPA2006-2014/About.
83 Moeller2011, S.148.

mögenswerten durchgeführt wird“[84]. Ein Jahr darauf wurde von der *Cohen Commission* ein Lagebericht zum Management Reporting zur Umsetzung der Internal Control als Teil des Jahresberichts vorgeschlagen, welcher von der SEC als verpflichtend für alle an der Börse notierten Unternehmen eingeführt werden sollte. Jedoch aufgrund von mehrfacher Kritik, bezüglich der hohen Kosten und Irrelevanz der Inhalte, wurde dieses Vorhaben nicht umgesetzt. Bis zum Jahr 1985 wurde Internal Control vor allem in der Entwicklung und Verfeinerung der Prüfstandards (*Statements on Auditing Standards*) und Durchführung von Studien zur Evaluierung von internen Kontrollen weitergeführt, bis eine hohe Anzahl an Firmenpleiten und angeblichen Prüfungsmisserfolgen dazu führten, dass aufgrund von vermehrten Verhandlungen im Untersuchungsausschuss ein Gesetz zur Behebung von Finanz-Berichterstattungsdelikten und zur Sicherstellung der Wirksamkeit der internen Kontrollen geschrieben wurde, welches jedoch nie umgesetzt wurde.[85]

“*The National Commission on Fraudulent Financial Reporting, known as Treadway Commission, was created in 1985 by the joint sponsorship of the AICPA, American Accounting Association, FEI, IIA and Institute of Management Accountants (IMA, formerly the National Association of Accountants). The Treadway Commission had as its major objective to identify the causal factors of fraudulent financial reporting and to make recommendations to reduce its incidence. The Commission’s report, issued in 1987, included recommendations for management and boards of directors of public companies, the public accounting profession, the SEC and other regulatory and law enforcement bodies, and academics.*”[86] Mit der Gründung der Treadway Commission haben fünf Vertreter von unterschiedlichen Berufsständen des privaten Sektors mit dem Ziel zusammengefunden, jene Faktoren zu finden, die die Fälschung der Finanzberichterstattung oder betrügerisches Verhalten möglich machen. Zwei Jahre darauf wurde der *Report on Fraudulent Financial Reporting* veröffentlicht, in dem eine Reihe von Empfehlungen zum internen Kontrollwesen enthalten sind, welche die Bedeutung des Kontrollumfelds, Verhaltenskodizes, kompetente und engagierte Prüfungsausschüsse und eine aktive und objektive interne Revision hervorhebt. „*An array of concepts and views of internal control has developed over the years, expressed in proposed legislation, regulation, professional standards and guidelines, public and private reports, and a substantial and diverse body of academic literature. (…) They contain different definitions of internal control, disparate views on the role of internal control in an entity and how it should be established, and varying opinions on how internal control effectiveness should be determined.*”[87] Deshalb wurde im Jahr 1991 vom *Committee of Sponsoring Organizations* (COSO) *of the Treadway Commission* das *Internal Control – Integrated Framework* veröffentlicht, welches “*was initiated to provide a common understanding of internal control among all parties and to assist management to exercise*

[84] Klawatsch1995, S.6.
[85] Vgl. im Folgenden Klawatsch1995, S.5ff.; Moeller2011, S.148ff. und COSO1994, S.93ff.
[86] COSO1994, S.96.
[87] COSO1994, S.98.

better control over an enterprise."[88] Dieses Framework wird weltweit von Wirtschaftsprüfern und Unternehmen anerkannt und eingesetzt. Aufgrund der Änderungen hinsichtlich Wirtschaft und Technologie wurde 2010 ein Update von COSO angekündigt, um dem immer komplexer werdenden Umfeld für Unternehmen und darin der Implementierung und Bewertung von Internal Control gerecht zu werden. Am 14. Mai 2013 wurde das COSO Internal Control – Integrated Framework in einer neuen Version herausgegeben.[89]

4.1.2 American Accounting Association

Die *American Accounting Association* wurde im Jahr 1916 gegründet und ist bis dato die größte Gemeinschaft an Bilanzbuchhaltern in der Wissenschaft (25% aller Mitglieder sind von außerhalb der USA) und „*recognizes its mission to be the "premier forum for scholarly interchange in accounting." The Association acknowledges that its members share a number of common values including the importance of integrity, objectivity, a sense of community, open communications, respect for others, high ethical values and behaviors, an increasingly global perspective, and an obligation to serve important stakeholders, including the broader society within which we operate. This statement is an expression of the values we share and, while not intended to be enforceable, is designed to serve as a broad guide to the behavior we expect of each other*."[90] Als weltweites Netzwerk investiert die AAA vor allem in die Forschung und Publikation in Bezug auf die Rechnungslegung und bietet für Mitglieder Zugang zu diesen Publikationen, wie Zeitschriften und Newslettern, es werden Treffen organisiert und ein breites Spektrum an Ressourcen für Lehre, Forschung und Praxis geboten.[91]

4.1.3 American Institute of Certified Public Accountants

Das *American Institute of Certified Public Accountants* (AICPA) wurde im Jahr 1887 als *American Association of Public Accountants* (AAPA) als ein Verband von Staatsgesellschaften gegründet, jedoch schon vor der offiziellen Gründung wurden regelmäßig Ausschüsse abgehalten, welche Regeln und Vorschriften erarbeiteten und im Anschluss von der *Securities and Exchange Commission* (SEC) herausgegeben bzw. verwendet werden. Erst im Jahr 1936 „*the society was merged into the Institute (…) and, at that time, the In-*

[88] COSO1994, S.98.
[89] Vgl. im Folgenden COSO1994, S.97f.; Klawatsch1995, S.7f.; KPMG26_2013/05, S.1 und COSO.org11/2010, S.1.
[90] AAA1998-2014/Statement of Responsibilities, Preamble.
[91] Vgl. im Folgenden AAA1998-2014/Join und AAA1998-2014/About.

stitute agreed to restrict its future members to CPAs"[92] (*Certified Public Accountants*). Das erste *Statement on Auditing Standards* (SAS no.1) war ein wesentlicher Bestandteil für die Durchführung der Prüfung von Jahresabschlüssen und leistete einen wichtigen Beitrag zur Definition von Internal Control und wurde in den Folgejahren auf die Unterscheidung zwischen *Internal Administrative Controls* und *Internal Accounting Control* erweitert[93]:

„*Administrative Control includes, but is not limited to, the plan of enterprise and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the enterprise and is the starting point for establishing accounting control of transactions*. (…)

Accounting Control comprises the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that:

a. *Transactions are executed in accordance with management's general or specific authorization.*
b. *Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statement and (2) to maintain accountability for assets.*
c. *Access to assets is permitted only in accordance with management's authorization.*
d. *The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.*"[94]

Diese Definition von Internal Control wurde über die Jahre nur selten verändert und neu interpretiert, aber es gab von verschiedenen CPA Unternehmen, sowohl von der SEC als auch dem AICPA, weitere Guidelines, Frameworks und dadurch auch abgewandelte Interpretationen zum Internal Control, welche auch zu der heutigen Gesetzgebung, vor allem im *Sarbanes-Oxley Act*, geführt haben. Das AICPA hat heute über 394.000 Mitglieder in 128 Ländern der Welt und gilt damit als der weltweit größte Verband an CPAs, bietet eine große Auswahl an Prüfungsstandards und eine vereinheitlichte Zertifizierung für Wirtschaftsprüfer – mit den Zielen, die Interessen der Wirtschaftsprüfer zu schützen und zu fördern, ein höchstmögliches Niveau der einheitlichen Zertifizierungs- und Zulassungsstandards der CPAs zu gewährleisten, die Förderung des Bewusstseins der Öffentlichkeit und damit das Vertrauen, die Integrität, Objektivität, Kompetenz und Professionalität zu wahren und den Aufbau professioneller Standards zu leisten, um die Mitglieder in ihrem

[92] AICPA2010/History.
[93] Vgl. im Folgenden AICPA2010/History; Root1998, S.76 und Moeller2011, S.148f.
[94] Moeller2011, S.148.

beruflichen Verhalten und deren Leistung kontinuierlich zu verbessern und damit die Überwachung dieser Leistung und die Einhaltung aktueller Standards und Anforderungen zu gewährleisten.[95]

4.1.4 Financial Executives International

Financial Executives International (FEI) wurde im Jahr 1931 als *Controller Institute of America* gegründet, um den Beruf des Controllers zu definieren und die Bedürfnisse und Interessen der Mitglieder in Bezug auf die Führungskräfte durch Ideenaustausch und einer Zusammenarbeit mit der Regierung, um die Gesamtwirtschaft zu verbessern. Durch die Weltwirtschaft wurde im Jahr 1969 nicht nur der Name, sondern auch die Philosophie des Verbandes geändert und öffnete im Jahr 2000 die Mitgliedschaften für alle Finanzführungskräfte auf der ganzen Welt. Primär stellt das FEI lokale und internationale Foren zur Verfügung, in welchen die Mitglieder Wissen aufbauen und nationale und internationale Politische Debatten führen können, um bei fundierten Geschäftsentscheidungen zu unterstützen.[96]

4.1.5 The Association of Accountants and Financial Professionals in Business

The Association of Accountant and Financial Professionals in Business (IMA) wurde im Jahr 1919 als *National Association of Cost Accountants* gegründet, um das Wissen und die Professionalität von Betriebsbuchhaltern zu fördern und eine höhere Akzeptanz und Verständnis für diese Berufsgruppe beim Management zu erreichen. Die Abkürzung IMA kommt von einer Namensänderung im Jahr 1991 zu *Institute of Management Accountants* und bietet ein Zertifiziertes Programm für Buchhalter (CMA) und Financial Manager (CFM). Im Jahr 1983 wurden die ersten *Standards of Ethical Conduct of Management Accountants* herausgegeben, welche zu diesem Zeitpunkt die ersten *Standards of Ethic* für diese Berufsgruppe darstellten. Bis dato zählt IMA 70.000 Steuerberater und Finanzexperten zu ihren Mitgliedern und bietet durch ein strenges Zertifizierungsprogramm einen Berechtigungsnachweis für Finanzberufe, stellt ein umfangreiches Bildungsprogramm zur Verfügung, um professionelle Kenntnisse zu erweitern und das Führungspotenzial ihrer Mitglieder zu erhöhen, und fördert die Forschung im Finanzsektor.[97]

---

[95] Vgl. im Folgenden AICPA2006-2014/About und Moeller2011, S.149.
[96] Vgl. im Folgenden FEI2014/History und FEI2014/About.
[97] Vgl. im Folgenden IMA1997-2014/Mission und IMA1997-2014/History.

4.1.6 Institute of International Auditors

Das *Institute of International Auditors* (IIA) wurde im Jahr 1941 als internationaler Berufsverband für Interne Revisoren gegründet und legt durch die Herausgabe des ersten Buches über die Interne Revision den Grundstein für das *International Professional Practices Framework* (IPPF), welches als konzeptioneller Rahmen und maßgeblicher Leitfaden für den Berufsstand und die weitere Zertifizierung zum Internen Revisor gilt. Die IPPF beinhalten, als Regelwerk für den Internen Revisor, die offizielle Definition der Internen Revision, den *Code of Ethics* und die internationalen Standards für die berufliche Praxis der Internen Revision, „diese Bestimmungen beschreiben die Eigenschaften, Verfahren und Aktivitäten, die für die berufliche Praxis der Internen Revision wesentlich sind.“[98] Als Erweiterung und zusätzliche Hilfestellung zur Umsetzung der verbindlichen Leitlinien des IPPF dienen die *Practice Advisories*, *Position Papers* und *Practice Guides*, als Erklärungen, deren Einhaltung nur empfohlen wird, um einen größeren Spielraum bei der Umsetzung zu ermöglichen. Des Weiteren bietet die IIA seit Jahren die weltweit gültige Ausbildung zum einzig anerkannten *Certified Internal Auditor* (CIA) als einheitliche Zertifizierung an und bietet damit einen Nachweis über alle Bereiche des die Interne Revision umfassenden Wissens. Das Anforderungsprofil und die Aufgabenstellung eines Internen Revisors sind damit auf eine weltweit einheitliche Basis gestellt. Neben dem CIA werden vier weitere Zertifizierungsprogramme und ein Qualifizierungskurs angeboten, um der stetigen Veränderung der Wirtschaft Rechnung zu tragen[99]:

- „*Certification in Control Self Assessment* (CCSA) wurde speziell für Praktiker des *Control Self Assessment* entwickelt. Bei der Auseinandersetzung mit dem geforderten Wissen auf dem Gebiet von Risiko- und Kontrollmodellen werden Konzepte vermittelt, die für eine effektive Nutzung des CCSA als Unterstützung der Kunden bei der Zielerreichung von grundlegender Bedeutung sind.“[100]
- *Certified Financial Services Auditor* (CFSA) stellt eine Zertifizierung speziell für Interne Revisoren im Finanzdienstleistungssektor dar, wie zum Beispiel aus Banken, Kreditgesellschaften und Versicherungen.
- *Certification in Risk Management Assurance* (CRMA) wird für Interne Revisoren im Risikomanagement, mit Verantwortung und Erfahrung für die Bereitstellung von Risikosicherung, Governance-Prozessen, Qualitätssicherung und Control Self Assessment bereitgestellt.
- *Certified Government Auditing Professional* (CGAP) ist speziell für Interne Revisoren des öffentlichen Bereichs entwickelt worden und soll spezielles Wissen über die Ausprägungen und Anforderungen im öffentlichen Bereich vermitteln.

---

[98] IIA2008, S.28.
[99] Vgl. im Folgenden IIA2008, S.28 sowie S.76f.; IIA2014/About; IIA2014/Certification und IIA2014/Standards-and-Guidance.
[100] IIA2008, S.78 und S.79.

- *Qualification in Internal Audit Leadership* (QIAL) soll Internen Revisoren, mit dem Ziel, eine führende Position im eigenen Unternehmen zu übernehmen, dabei unterstützen, Fähigkeiten aufzubauen oder zu verbessern, die eine aktuelle Führungsposition rechtfertigen.[101]

[101] Vgl. im Folgenden IIA2008, S.77ff. und IIA2014/Certification.

4.2 Internal Control – Integrated Framework

4.2.1 Definition von Internal Control nach dem Committee of Sponsoring Organizations of the Treadway Commission

„Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."[102]

Den Grundstein für das interne Kontrollsystem nach *COSO* legt ein einfaches Konzept, dem zufolge Internal Control als Prozess zu verstehen ist, welcher von Menschen beeinflusst wird, nur messbare Gewissheit (und niemals absolute Gewissheit) über die Unternehmensprozesse sicherstellen kann und auf die Erreichung von Zielen ausgerichtet ist, wobei Internal Control an die Unternehmensstruktur abgepasst werden kann und damit für das gesamte Unternehmen sowie bestimmte Teilbereiche angewendet werden kann. Damit bietet Internal Control nach COSO eine Grundlage für verschiedene Anwendungsarten in den verschiedenen Organisationen, Branchen und Regionen und wird als ein Konzept verstanden, das zum Design, zur Implementierung und Durchführung von internen Kontrollen und zur Bewertung der Wirksamkeit des internen Kontrollsystems beitragen soll.[103]

Die nach dem COSO Internal Control – Integrated Framework festgelegten drei Zielkategorien sind auf die separaten Aspekte der internen Kontrollen abgestimmt und umfassen

- die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (*Operations Objectives*),
- die Zuverlässigkeit der Berichterstattung (*Reporting Objectives*) und
- die Einhaltung der entsprechenden Gesetzte und Verordnungen (*Compliance Objectives*).

Dabei kann ein bestimmtes Ziel unter mehrere Kategorien fallen; und man kann diese Zielkategorien als die Erwartung in Internal Control verstehen, also dass eine Organisation mit hinreichender Sicherheit die Ziele in Bezug auf die Kategorien erreichen kann. Die Erreichung dieser Ziele hängt davon ab, wie die Aktivitäten innerhalb der Kontrollen eines Unternehmens durchgeführt werden. Dabei kann man nicht aus einem Ereignis oder Umstand schlussfolgern, sondern man muss Internal Control als einen dynamischen und sich wiederholenden Prozess ansehen, bei welchem die Aktivitäten eines Unternehmens mit Kontrollen zu durchdringen sind und sich darin die Art und Weise der Managementführung in den einzelnen Verfahren und bestehenden Richtlinien widerspiegeln. Internal

[102] COSO2013, S.1.
[103] Vgl. im Folgenden COSO1994, S.13 und COSO2013, S.1f.

Control muss also in die Geschäftsprozesse und -aktivitäten eingebettet sein, um effektive und effiziente Kontrollen zu gewährleisten. „*Internal control is effected by the board of directors, management, and other personnel. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put actions in place to achieve specified objectives.*"[104] Demnach ist vor allem die Einstellung des Managements ("*tone at the top*") ein wichtiges Element für Internal Control, um die Bedeutung für das Unternehmen und die erwarteten Verhaltensstandards festzulegen. „*Each individual brings to the workplace a unique background and ability, and each has different needs and priorities. These individual differences can be inherently valuable and beneficial to innovation and productivity, but if not properly aligned with the entity's objectives they can be counterproductive.*"[105] Somit müssen die Verantwortlichkeiten und Rollen, gemeinsam mit den konkreten Aufgaben und Zielen des Unternehmens übereinstimmen und auch konkret kommuniziert werden. Erschwerend kommt hinzu, dass Einheiten entlang verschiedener Dimensionen strukturiert werden können, auf verschiedenen geographischen Märkten arbeiten, in unterschiedlichen Geschäftsbereichen und Betriebseinheiten aufgeteilt sind oder ausgelagerte Dienstleistungen nutzen, wobei „*Internal control can be applied, based on management's decisions and in the context of legal or regulatory requirements, to the management operating model, legal entity structure, or a combination of these.*"[106] [107]

„*The term "reasonable assurance" rather than "absolute assurance" acknowledges that limitations exist in all systems of internal control, and that uncertainties and risks may exist, which no one can confidently predict with precision. Absolute assurance is not possible*."[108] Damit soll klargestellt werden, dass hinreichende Sicherheit nicht bedeutet, dass ein Unternehmen alle seine Ziele erreicht. Eine wirksame interne Kontrolle erhöht ausschließlich die Wahrscheinlichkeit zur Zielerreichung, wobei selbst diese durch Beschränkungen, die in allen Internal-Control-Systemen zu finden sind, wie zum Beispiel menschliches Versagen, die Unsicherheit hinter den eigenen Urteilen und die Auswirkungen von externen Ereignissen, die außerhalb von Kontrollen wirken; im Speziellen wenn das Management in der Lage ist, „*to override controls, the entire system may fail*"[109], obwohl das interne Kontrollsystem zur Vermeidung und Aufdeckung solcher Vorfälle beitragen soll.[110]

[104] COSO2013, S.3.
[105] COSO2013, S.3.
[106] COSO2013, S.4.
[107] Vgl. im Folgenden COSO2013, S.2ff.; Ramos2006, S.37ff. und Klawatsch1995, S.10f.
[108] COSO2013, S.4.
[109] COSO2013, S.4.
[110] Vgl. COSO2013, S.4.

Abb. 9 Internal Control Cube[111]

Das COSO Internal Control – Integrated Framework wird in drei Dimensionen aufgeteilt, wobei die dritte Dimension sowohl das gesamten Unternehmen oder den Konzern als auch die einzelnen betrieblichen Einheiten und Aktivitäten darstellt. Im zweiten Teil werden bestimmte Ziele vorgegeben, welche ein Unternehmen in Bezug auf das vorhandene interne Kontrollsystem erreichen muss und im dritten Teil werden die fünf Dimensionen zur Zielerreichung festgelegt, wobei es besonders wichtig ist die Wechselbeziehung dieser fünf Komponenten zu verstehen, „*COSO envisions these individual components as being tightly integrated with each other in a nonlinear fashion. Each component has a relationship with and can influence the functioning of every other component.*"[112] Diese dreidimensionale Darstellung soll verdeutlichen, dass alle fünf Komponenten des internen Kontrollsystems zur Zielerreichung für das gesamte Unternehmen, als auch für die einzelnen betrieblichen Einheiten und Aktivitäten relevant sind. Diese direkte Beziehung zwischen den Dimensionen lässt sich grafisch durch einen Würfel darstellen, wobei die drei Zielkategorien durch die Spalten, die fünf Dimensionen zur Zielerreichung durch die Zeilen und die Unternehmensstruktur durch die dritte Dimension des Würfels dargestellt werden; damit wird deutlich, dass jede der fünf Komponenten sich mit allen drei Zielkategorien überschneiden kann und der Einfluss für das gesamte Unternehmen relevant ist. „*Internal control is dynamic, iterative, and integrated process. (…) Thus, internal control is not a linear process where one component affects only the next. It is an integrated process in which components can and will impact another.*"[113] [114]

[111] COSO2013, S.5
[112] Ramos2006, S.36.
[113] COSO2013, S.6.
[114] Vgl. im Folgenden COSO1994, S.16ff.; COSO2013, S.5f.; Bungartz2011, S.47; Ramos2006, S.36 und Löffler2011; S16.

4.2.2 Objectives

„*Management, with board oversight, sets entity-level objectives that align with the entity's mission, vision, and strategies. These high-level objectives reflect choices made by management and board of directors about how the organization seeks to create, preserve, and realize value for its stakeholders. Such objectives may focus on the entity's unique operations needs, or align with laws, rules, regulations, and standards imposed by legislators, regulators, and standard setters, or some combination of the two. Setting objectives is a prerequisite to internal control and a key part of the management process relating to strategic planning.*"[115] Das COSO Internal Control – Integrated Framework gliedert die Ziele eines Unternehmens in drei Kategorien, ***Operations***, ***Reporting*** und ***Compliance***.[116]

- „*An objective in one category may overlap or support an objective in another.(…)*
- *The category in which an objective falls may vary depending on the circumstances. (…)*
- *Operations and internal reporting objectives are based on the organization's preferences, judgments, and choices. These objectives vary widely among entities simply because informed and competent people may select different objectives.*"[117]

Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (*Operations Objectives*)

Operationale Ziele beziehen sich auf die Verwirklichung der wesentlichen Ziele für die Existenz eines Unternehmens und hängen von den Entscheidungen des Managements in Bezug auf die Verwaltung, die Betriebsmodelle, industrielle Überlegungen und die Leistung des Unternehmen ab und sollen die Verbesserung von Effektivität und Effizienz bei der Erreichung der Gesamtziele sicherstellen. Demnach kann für alle Unternehmen die Verbesserung der finanziellen Leistung, Produktivität, Qualität, Umweltpraktiken, Innovation und Kunden- und Mitarbeiterzufriedenheit als Grundpfeiler für die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit zusammengefasst werden. Ein wichtiger Teil der **Operations Objectives** umfasst die Sicherung der Vermögenswerte, welche den Schutz und die Erhaltung der Vermögenswerte eines Unternehmens umfasst und die Grundlage für die Risikobewertung in Bezug auf deren Sicherung und damit die Auswahl und Entwicklung von Kontrollen erfordert, um dieses Risiko zu minimieren. „*Laws, rules, regulations, and external standards have created an exception that management reporting on internal control includes controls relating to preventing and detecting unauthorized acquisition, use, or disposition of entity assets.*"[118] [119]

[115] COSO2013, S.6.
[116] Vgl. COSO2013, S.7.
[117] COSO2013, S.10.
[118] COSO2013, S.7.

Zuverlässigkeit der Berichterstattung (*Reporting Objectives*)

Reporting Objectives beziehen sich auf die Erstellung von Berichten für ein Unternehmen zur Nutzung durch Organisationen und Interessensgruppen über finanzielle und nichtfinanzielle, interne und externe Berichterstattung, welche sich durch interne Anforderungen in Reaktion auf die strategische Ausrichtung, Betriebspläne und Leistungskennzahlen auf verschiedenen Ebenen in der internen Berichterstattung beziehen oder welche in erster Linie durch Vorschriften und Standards von Regulierungsbehörden und Normungsgremien in der externen Berichterstattung ausgesteuert werden.

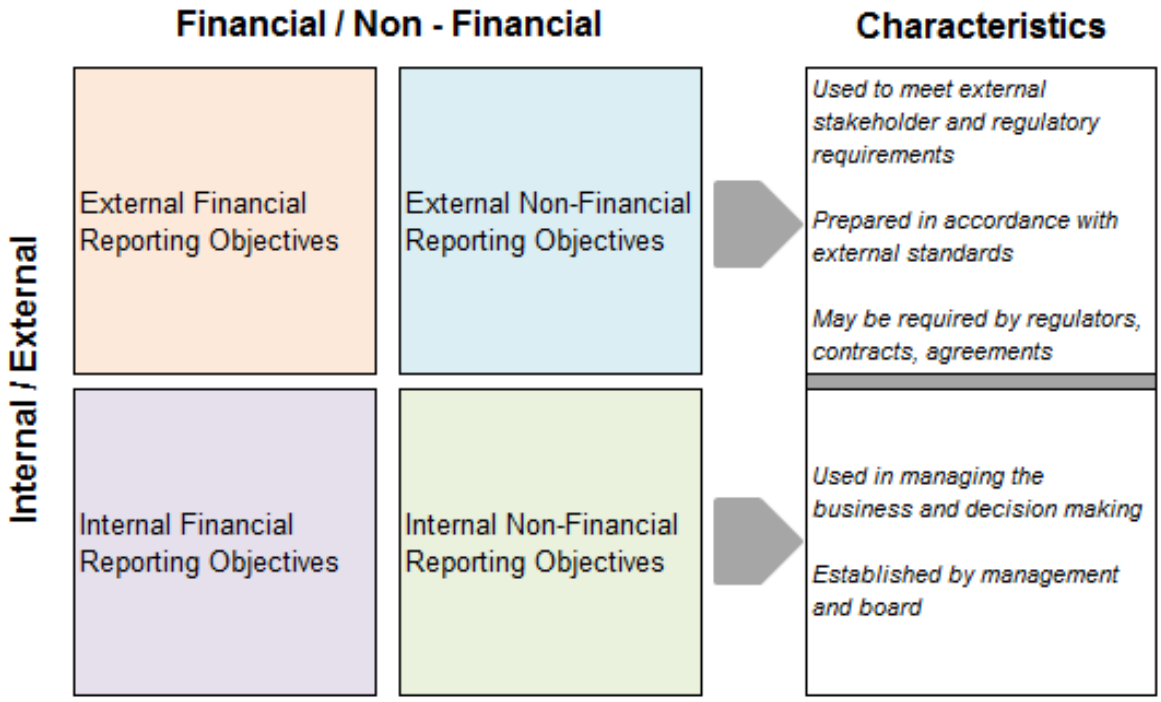

Abb. 10 Zusammenhang zwischen den Unterkategorien der *Reporting Objectives*[120]

„*Entities need to achieve* ***external financial reporting objectives*** *to meet obligations to and expectations of stakeholders.*“[121] Der wichtigste Teil der externen Finanzberichterstattung umfasst den Jahresabschluss, der einem Unternehmen den Zugang auf den Kapitalmarkt ermöglicht und damit entscheidend für die Verleihung von Verträgen im Umgang mit Lieferanten, Investoren, Analysten und Gläubiger ist und welcher expliziten Regeln, Vorschriften und externen Normen zur Erstellung folgt. „N*on-financial reporting*

[119] Vgl. COSO2013, S.7.
[120] Vgl. COSO2013, S.9.
[121] COSO2013, S.8.

requirements as set forth by regulations and standards for management reporting on the effectiveness of internal control over financial reporting are part of ***external non-financial reporting objectives***"[122]; und um ein Unternehmen zu verwalten, müssen alle als notwendig erachteten Informationen an das Management und den Aufsichtsrat herangetragen werden, um diese bei der Entscheidungsfindung und Bewertung der Aktivitäten und Leistungen des Unternehmens zu unterstützen. „***Internal reporting objectives*** *are based on preferences and judgments of management and the board. Internal reporting objectives vary among entities because different organizations have different strategic directions, operating plans, and expectations.*"[123] [124]

Einhaltung der entsprechenden Gesetzte und Verordnungen (*Compliance Objectives*)

„*As part of specifying* ***compliance objectives****, the organization needs to understand which laws, rules, and regulations apply across the entity*"[125] und in Übereinstimmung mit diesen handeln. Damit muss sichergestellt werden, dass Gesetze, Regelungen und Vorschriften in allen Aktivitäten und Maßnahmen angewendet werden und diese in die für das Unternehmen festgelegten Ziele integriert sind. Die meisten Unternehmen haben darüber hinaus ein höheres Niveau an Regeln als durch Gesetze und Verordnungen festgelegt, um damit die Diskretion und Lage in Bezug auf die Performance zu wahren.[126]

[122] COSO2013, S.8.
[123] COSO2013, S.8.
[124] Vgl. COSO2013, S.8f.
[125] COSO2013, S.9.
[126] Vgl. COSO2013, S.9f.

4.2.3 Components and Principles

4.2.3.1 Control Environment

Das Kontrollumfeld bildet die Basis jeder wirksamen internen Kontrolle, es verleiht dem Unternehmen Struktur durch Integrität und ethische Werthaltung. Dabei wird das Kontrollumfeld durch die Unternehmenskultur, also die Werthaltung und das Verhalten aller Beteiligten, widergespiegelt. Die Vorbildfunktion des Managements („*Tone at the top*“) durch das gelebte Verhalten, formalisierte Normen und auch Strafmaßnahmen bei Normverstößen kann teilweise das Verhalten der Mitarbeiter beeinflussen.[127]

- *„The Organization demonstrates a commitment to integrity and ethical values“*[128]

Um die Unternehmensstruktur und -kultur festzulegen, können betriebswirtschaftliche Werkzeuge verwendet werden, wie das *Mission Statement*, der *Code of Conduct*, Rundschreiben, Arbeitsanweisungen, direkte Kommunikation im jeweiligen Bereich, Managemententscheidungen und regelmäßige Informationen durch die Unternehmensleitung, nicht nur um mitzuteilen, welche Erwartungen außerhalb der lokalen Gesetzgebung und Normen an die Beteiligten gestellt werden, sondern auch um in komplexen Situationen oder bei schwierigen Entscheidungen durch eine Vorbildwirkung die Haltung und Einstellung der betroffenen Beteiligten zu beeinflussen („*Tone at the top*“). Zusätzlich sollen Verhaltensnormen die Organisation dazu anleiten, Aktivitäten und Entscheidungen zielgerichtet zu treffen, damit zeigen, was richtig oder falsch ist, als Orientierungshilfe zur Risikoerkennung und die geltenden Gesetze, Normen, Vorschriften, sowie die soziale Verantwortung des Unternehmens widerspiegeln. („*Standards of Conduct*“) Je nach Größe des Unternehmens wird dieses Umfeld informell oder formell gebildet und kann auch zu Abweichungen führen. Vor allem bei einer mangelhaften Kommunikation zwischen den unterschiedlichen Ebenen kann es zu Abweichungen kommen. Deshalb sollte sichergestellt werden, dass das Senior Management über wichtige Schritte informiert ist und Mitarbeiter die Möglichkeit haben, Fragen und Bedenken zu äußern. Interne Schulungen, Audits, Prozessüberprüfungen und periodische Anpassungen an die sich verändernde Umwelt können diesem Umstand entgegenwirken. („*Adherence and Deviations*“)[129]

- *„The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.“*[130]

Der Vorstand eines Unternehmen sollte die Verantwortung für interne Kontrollen von seinem Standpunkt aus vertreten und in alle Organisationseinheiten tragen, dazu muss ein ausreichendes Wissen und Verantwortungsbewusstsein vorhanden sein; und der Vor-

---

[127] Vgl. Jenal2006, S.28f.
[128] COSO2013, S.33.
[129] Vgl. im Folgenden COSO2013, S.33f. sowie 36ff. und Arwinge2013, S.43.
[130] COSO2013, S.39.

stand sollte unabhängig von der Unternehmensleitung fungieren, um Entscheidungen objektiv treffen zu können. („*Authorities and Responsibilities*“) Eine periodische Überprüfung der eigenen Verantwortungsfelder, um angemessene Maßnahmen ergreifen zu können („*Independence and Relevant Expertise*“), ist vor allem in Hinblick auf die Endverantwortung für die Implementierung, das Design und die Durchführung der internen Kontrollen relevant. („*Oversight by the Board of Directors*“)[131]

- *“Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives”*[132]

Ein Unternehmen hat viele verschiedene Distributionswege, um neue Produkte und Services am Markt zu etablieren, die optimale Marktpositionierung zu erreichen, Produktionsstätten, Kundendienste oder andere operative Aspekte, welche vor allem in internationalen Unternehmen in verschiedene Tochtergesellschaften mit unterschiedlichen geografischen Strukturen und einer großen Anzahl an Dienstleistungsunternehmen aufgeteilt sind. Um eine effektive Umsetzung des internen Kontrollsystems sicherzustellen, müssen diese Wege klar strukturiert und in regelmäßigen Abständen evaluiert werden. („*Organizational Structures and Reporting Lines*“) Für jeden Mitarbeiter bis zum Vorstand sollten die Verantwortlichkeiten in derselben Struktur festgelegt werden, um den Zielen des Unternehmens entsprechende Entscheidungen treffen zu können und dem Management die Möglichkeit zu geben, den jeweiligen Mitarbeitern die Risiken und Chancen des Unternehmens aufzuzeigen, um zielgerichtet zu arbeiten und Aufgaben innerhalb des Verantwortungsbereichs zu delegieren. („*Authorities and Responsibilities*“) Diese Delegation sollte in der jeweiligen Struktur nur im Umfang der Zielerreichung definiert und mit klaren Grenzen eingeschränkt werden. Manche Aufgaben sollten nur getrennt vergeben werden, um das Risiko von unangemessenem Verhalten zu vermeiden und den Bezug zwischen Kontrolle und Gegenkontrolle zu erhalten. In den meisten Unternehmen können diese Grenzen durch die gelebte IT-Landschaft, zum Beispiel mit Zugangsbeschränkungen oder Rechtevergabe, umgesetzt werden. („*Limitation of Authority*“)[133]

- *„The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives“*

Durch die Definition von Richtlinien werden innerhalb des Unternehmens klare Anforderungen und Grundprinzipien aufgestellt, um die notwendigen Fähigkeiten und Verhaltensweisen zur Erreichung der Unternehmensziele vorzugeben. Damit wird die Basis für die Bewertung von Mängeln und Fehlern geschaffen, um zeitgerecht risikoeindämmende Maßnahmen einzuleiten. („*Policies and Practices*“) Zu beachten ist dabei, dass jeder Beteiligte die notwendige Kompetenz und Qualifikation zur Durchführung der übertragenen

[131] Vgl. COSO2013, S.39ff.
[132] COSO2013, S.44.
[133] Vgl. COSO2013, S.45ff.

Aufgabe besitzen sollte („*Evaluate Competence*“), was bereits bei der Einstellung eines Mitarbeiters – gleichgültig, auf welcher Ebene oder Führungsposition – eine große Rolle spielt. Ein Mitarbeiter sollte seine Zugehörigkeit zur Unternehmenskultur zeigen, alle relevanten Trainings und ausreichend individuelle Information und Hilfestellung zur Verfügung gestellt bekommen. In periodischen Abständen sollten die Zielerreichung überprüft und Anreize zur Stärkung des gewünschten Verhaltens und zur Motivation eingerichtet werden. („*Attracting, Developing, and Retaining Individuals“)* Ein Teil der Aufstellung von Richtlinienkompetenz ist die kontinuierliche Identifizierung und Bewertung von Vorsorgeplänen in Zusammenhang mit der Delegation von Verantwortungen für interne Kontrollen. Dazu sollten die Auswirkungen und das Risiko bei dauerhaftem oder vorübergehendem Ausfall einer Position in allen Unternehmensbereichen bewertet und bestimmt werden. („*Plans and Prepares for Succession*“)[134]

- „*The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives*“[135]

Der Unternehmensvorstand macht den Geschäftsführer für das Verständnis der Risiken und Chancen des Unternehmens und die Umsetzung des erforderlichen internen Kontrollsystem verantwortlich, der wiederum die Gestaltung, Umsetzung, Durchführung und Bewertung der internen Kontrollen gemeinsam mit dem Senior Management durchführt, um die Verantwortung für die internen Kontrollen auf allen Ebenen der Organisation zu etablieren. („*Accountability for Internal Control*“) Dabei unterstützen Anreize und Belohnungen sowie konkrete Ziele und Vorgaben die Wirksamkeit des internen Kontrollsystems, soweit diese auf die Ziele des Unternehmens angepasst sind, sich dynamisch weiterentwickeln und deren Resultate regelmäßig überprüft werden. („*Performance Measures, Incentives, and Rewards*“, „*Pressures“* und *„Performance Evaluation and Reward*“)[136]

4.2.3.2 Risk Assessment

Ausgehend von den Unternehmenszielen sollen Mechanismen eingerichtet sein, welche der Identifizierung und Steuerung von Risiken dienen. Um eine Risikobeurteilung aller externen und internen Risiken vornehmen zu können, müssen die nach *COSO* definierten Ziele des Unternehmens festgelegt sein, dabei wird in Anlehnung an die Dimensionen eines Kontrollsystems nach *COSO* zwischen operativen Unternehmenszielen, finanziellen Zielen und Zielen betreffend die Einhaltung von Gesetzen und Vorschriften unterschie-

[134] Vgl. COSO2013, S.49ff.
[135] COSO2013, S.53.
[136] Vgl. COSO2013, S.54ff.

den. Erst dann kann man alle Risiken beurteilen, denen ein Unternehmen ausgesetzt ist und die die Erreichung der Unternehmensziele gefährden.[137]

- „*The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives*“[138]

Eine Voraussetzung für die Risikobewertung, jedoch nicht Teil des internen Kontrollprozesses, ist die Festlegung von Zielen und diese auf verschiedenen Ebenen des Unternehmens zu verknüpfen, um die strategische Ausrichtung festzulegen. Diese Ziele bilden die Grundlage für die Umsetzung der Risikobewertungsansätze und die nachfolgenden Kontrollaktivitäten, welche in drei Kategorien gruppiert sind und im gesamten Unternehmen umgesetzt werden. Ziele, die Entscheidungen in Bezug auf das Tätigkeitsfeld, die Industrie oder das wirtschaftliche Umfeld des Unternehmens betreffen, unterstützen dabei, die gewünschte Leistung zu erreichen. („*Operations Objectives*“) Die Erreichung von gewünschter Unternehmensleistung geht mit allen Zielen in Bezug auf die Zuverlässigkeit, Aktualität und Transparenz von finanzwirtschaftlichen, nicht finanzwirtschaftlichen (Gesetze, Frameworks, Rundschreiben, Normen, usw.) und internen Berichterstattungen einher und bildet, jedes für sich, eine eigene Zielgruppierungskategorie. („*External Financial, Non-Financial and Internal Reporting*“) Als letzte Kategorie werden alle Ziele, die zur Aufdeckung von kriminellem Verhalten und anderen Vergehen dienen, zusammengefasst, welche aus der lokalen Gesetzgebung oder tatsächlichem kriminellen Verhalten abgeleitet werden. („*Compliance Objectives*“)[139]

- “*The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risk should be managed*”[140]

Die Risiken einer Organisation müssen auf allen Ebenen des Unternehmens mit allen Faktoren, wie dem Härtegrad, der Umlaufgeschwindigkeit, der Nachhaltigkeit, der Eintrittswahrscheinlichkeit und der Höhe des möglichen Verlustes des Risikos, identifiziert werden. („*Risk Identification*“) Dazu muss eine umfassende Analyse aller Waren, Dienstleistungen und Informationen und der damit verbundenen Auswirkungen und signifikanten Wechselwirkungen auf das Unternehmen, das Reporting und die Compliance-Aktivitäten erfolgen. („*Risk Analysis*“) Sobald die potenzielle Bedeutung von Risiken beurteilt wurde, können entsprechende Gegensteuerungsmaßnahmen ausgearbeitet werden, welche zu einer Verringerung der Höhe des Risikos (***Reduction***), keiner Steuerung des Risikos

[137] Vgl. Jenal2006, S.28ff.
[138] COSO2013, S.59.
[139] Vgl. COSO2013, S.62ff.
[140] COSO2013, S.59.

(***Acceptance***), einer Vermeidung des Risikos (***Avoidance***) oder zu einem Transfer des Risikos führen können (***Sharing***). („*Risk Response*“)[141]

- "*The organization considers the potential for fraud in assessing risks to the achievement of objectives*" [142]

Ein internes Kontrollsystem kann zur Aufdeckung und Verhinderung von Unregelmäßigkeiten, unberechtigten Einnahmen oder Ausgaben und Finanzfehlverhalten in Bezug auf die betrügerische Finanzberichterstattung beitragen, jedoch nicht zur Verhinderung von korruptem, illegalem Verhalten. Korruption hat einen beträchtlichen Einfluss auf das Kontrollumfeld und die externe Finanzberichterstattung des Unternehmens und muss zur Risikodefinition herangezogen werden. („*Types of Fraud*“) Die Unternehmensleitung ist bei der Nutzung von Kontrollen mit betrügerischen Absichten, wie persönliche Bereicherungen oder zur verbesserten Darstellung der finanziellen Unternehmenssituation, dazu angehalten Maßnahmen zu ergreifen, zu dokumentieren und an die entsprechenden Mitarbeiter offenzulegen. („*Management Override*“) Durch die Verwaltung von *Fraud*-Risiken kann durch die gesetzten Aktivitäten vom Management eine direkte Beurteilung des Risikos erfolgen, so entsteht durch die Offenlegung ein Anreiz, der den Druck im Unternehmen erhöht, unangemessene Handlungen zu unterlassen. („*Factors Impacting Fraud Risk*“) Sollten die bereits gesetzten Aktivitäten nicht ausreichen, kann die Eintrittswahrscheinlichkeit solcher Risiken mit betrügerischer Absicht durch andere interne Kontrollen oder eine Änderung der Geschäftsprozesse und betrieblichen Aktivitäten entgegengewirkt werden. („*Other Considerations in Fraud Risk Assessment*“)[143]

- "*The organization identifies and assesses changes that could significantly impact the system of internal control*" [144]

Bei der Risikoidentifizierung ist auf die Veränderungen der regulatorischen, wirtschaftlichen und physischen Umwelt des Unternehmens einzugehen, welche potenzielle Auswirkungen auf neue und bestehende, erworbene oder ausgegliederte Geschäftsfelder haben kann, ausgehend von schnellem Wachstum, neuen Technologien, Abhängigkeiten von ausländischen Regionen oder Änderungen im Management. („*Assessing Change*“)[145]

---

[141] Vgl. im Folgenden COSO2013, S.70ff. und Löffler2011, S.195.
[142] COSO2013, S.59.
[143] Vgl. COSO2013, S78ff.
[144] COSO2013, S.59.
[145] Vgl. COSO2013, S.83ff.

4.2.3.3 Control Activities

Kontrollrichtlinien und Kontrollverfahren sollen von der Unternehmensführung festgelegt sein. Kontrollaktivitäten sind auf allen Ebenen und in allen Bereichen eines Unternehmens vorzufinden und können unter anderem formeller oder informeller Art sein, manuell oder computergestützt erfolgen und lenkend, präventiv (***preventive***) oder nachgelagert (***detective***) wirken. Diese Steuerungs- und Kontrolltätigkeiten sind ein integrierter Bestandteil nahezu jeglicher Geschäftsaktivität und leisten einen wesentlichen Beitrag zur Erreichung der Unternehmensziele.[146]

- „*The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels*."[147]

Kontrollaktivitäten unterstützen alle Inhalte des internen Kontrollsystems, müssen jedoch mit allen Komponenten der Zieldefinition und Risikoevaluierung einhergehen, um sicherzustellen, dass die Kontrollaktivitäten bei der zielgerichteten Risikosteuerung die richtigen Maßnahmen leisten. („*Integration with Risk Assessment*") Dabei muss bedacht werden, dass jede Einheit spezifische Ziele und Implementierungsansätze hat, welche in den Kontrollaktivitäten berücksichtigt und an die jeweiligen Geschäftsprozesse angepasst werden müssen. („*Entity-Specific Factors*") In den einzelnen Geschäftsprozessen werden unterschiedliche Ziele und Sub-Ziele definiert, welche zu spezifischen Risiken und jeweiliger Risikosteuerung führen. Um diesen spezifischen Anforderungen gerecht zu werden, definiert das *COSO Internal Control – Integrated Framework* drei Hauptaussagen, die für jede Kontrollaktivität als Leitziele definiert sind. „***Completeness*** *– Transactions that occur are recorded. (…),* ***Accuracy*** *– Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing. (…),* ***Validity*** *– Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures (…)."*[148] („*Business Process Control Activities*") Dabei sollen die Kontrollaktivitäten so definiert sein, dass die Kontrollmaßnahmen der Art der geprüften Geschäftstätigkeit entsprechen und dass entweder Fehler vorab vermieden (preventive) um bereits erfolgte Fehler erfasst werden (detective). („*Types of Transaction Control Activities*") Viele Prozesse und auch Kontrollaktivitäten werden teilweise oder ausschließlich mit technologischen Hilfsmitteln durchgeführt und müssen dementsprechend überprüft werden. Dazu werden Kontrollen aufgesetzt, welche sicherstellen, dass die technologischen Hilfsmittel korrekt arbeiten und die Prozesse und Kontrollen dementsprechend vollständig, korrekt und gültig sind. („*Technology and Control Activities*") Zusätzlich gibt es Kontrollaktivitäten, die ausschließlich übergelagerte Aktivitäten betreffen. („*Control Activities at Different Levels*") Fasst man alle Anforderungen an Kontrollaktivitäten zusammen, ist eine Aufgabentrennung bereits auf Prozessebene für das interne Kont-

[146] Vgl. Jenal2006, S.28ff.
[147] COSO2013, S.87.
[148] COSO2013, S.91.

rollsystem von Vorteil, kann aber bei kleinen Unternehmen aufgrund geringerer Ressourcen teilweise nicht umgesetzt werden. („*Segregating Duties*“)[149]

- “*The organization selects and develops general control activities over technology to support the achievement of objectives*.” [150]

Bei allen Kontrollaktivitäten muss die Abhängigkeit und Verknüpfung von Geschäftsprozessen, automatisierten Kontrollaktivitäten und generellen technologiebasierten Kontrollen mit der technologischen Infrastruktur klar sein. („*Dependency between the Use of Technology in Business Processes and Technology General Controls*“) Des Weiteren müssen Zugriffsrechte für autorisierte Benutzer angepasst, entworfen und implementiert werden, vor allem um die Vermögenswerte des Unternehmens vor externen Bedrohungen zu schützen und die Entwicklung, den Erwerb und die Wartung der technologiebasierten Infrastruktur den Zielen des Unternehmens anzupassen. (“*Technology General Controls*”)[151]

- “*The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action*.” [152]

Als Basis für Kontrollaktivitäten sollten vom Management Prozessbeschreibungen dokumentiert und an die Mitarbeiter verteilt werden. Als Werkzeug dafür können Rundschreiben und Arbeitsanweisungen dokumentiert und in den verschiedenen Distributionskanälen verteilt werden. Im COSO Internal Control – Integrated Framework wird dazu definiert: „***Policies*** *reflect management's statement of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through management's actions and decisions. Procedures consist of actions that implement policy.*”[153] Diese Policies und Prozessbeschreibungen unterstützen bei der Implementierung von Kontrollaktivitäten während der Geschäftsaktivitäten in den täglichen Prozessschritten und definieren im Detail die Verantwortlichkeiten für die im Unternehmen gültigen Risiken und Ziele. Die Hauptinhalte dieser Prozessbeschreibungen definieren für die relevanten Kontrollaktivitäten die zeitliche Abfolge, Korrekturmaßnahmen im Fall von Abweichungen, Prozessverantwortliche und die erneute Bewertung durch den Vorgesetzten. („*Policies and Procedures*“)[154]

[149] Vgl. COSO2013, S.88ff.
[150] COSO2013, S.87.
[151] Vgl. COSO2013, S.97.
[152] COSO2013, S.87.
[153] COSO2013, S.101.
[154] Vgl. COSO2013, S.101.

4.2.3.4 Information and Communication

Alle Organisationsmitglieder sollen die Informationen erhalten, die zur Ausübung der Kontrolle notwendig sind. Relevante Informationen sind zu identifizieren, aufzuarbeiten und bezüglich Form und Zeithorizont so zu kommunizieren, dass es den jeweiligen Bereichen möglich ist, ihrer Verantwortung nachzukommen. Dabei sind externe und interne Informationen relevant, welche auch konkret ausformuliert werden können. Die Kommunikation muss dabei zum Informationsfluss beitragen, um sicherzustellen, dass die Unternehmensleitung klar kommuniziert, welche Verantwortung zu tragen ist.[155]

- „*The organization obtains or generates and uses relevant, quality information to support the functioning of internal control*.“[156]

Alle Komponenten eines funktionierenden internen Kontrollsystems sind von den zur Verfügung gestellten Informationen und deren Qualität abhängig. Daher ist es wichtig, das Kontrollumfeld regelmäßig anhand aller Informationen zu überprüfen. Vor allem, da die Risikobeurteilung abhängig von einem sich ständig veränderndem Umfeld ist und daher nur durch Informationen angepasst werden kann. Die Kontrolltätigkeiten sind wiederum abhängig von den Regelungen und Prozessbeschreibungen des Unternehmens, welche an alle Beteiligten verteilt werden müssen, denn die Überwachung kann nur mit den Informationen der Gegenproben erfolgen. („*Information Requirements*“) Die notwendigen Informationen werden über verschiedene Distributionswege, wie zum Beispiel E-Mail-Kommunikation, Berichtsysteme für interne Datenquellen, Regulierungsbehörden oder Soziale Netzwerke für externe Datenquellen, verteilt und zur Verfügung gestellt. („*Information from Relevant Sources*“) Diese Datenquellen bieten ein großes Spektrum an Daten, welche im Unternehmen erfasst und zu nutzbarer und umsetzbarer Information verarbeitet werden, die für die richtigen Personen in einer korrekten Form zum richtigen Zeitpunkt in einer gültigen Fassung nachvollziehbar zur Verfügung stehen müssen. („*Processing Data through Information Systems*“ und „*Information Quality*“)[157]

- “*The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*” [158]

Interne Kommunikation sollte zum Verständnis aller Beteiligten im Unternehmen für ihre jeweilige Verantwortung für interne Kontrollaufgaben beitragen und sowohl für die Mitarbeiter als auch für den Vorstand und die Unternehmensleitung sichergestellt sein, vor allem um die Ziele des Unternehmens in Hinsicht auf das interne Kontrollsystem zu erfüllen. („*Internal Control Communication*“ und „*Internal Control Communication with Board*“) Ab-

[155] Vgl. Jenal2006, S.28ff.
[156] COSO2013, S.105.
[157] Vgl. COSO2013, S.107ff.
[158] COSO2013, S.105.

gesehen von offiziellen internen Distributionswegen, muss eine offene Kommunikationspolitik im Unternehmen gelebt werden, um sicherzustellen, dass jeder Beteiligte Fehler, Missstände, oder Verbesserungsvorschläge kommunizieren kann und auch das Gefühl hat, dass seine Anregungen und Beschwerden geschätzt und respektiert werden. Das führt dazu, dass betrügerische Handlungen und Verletzungen von Unternehmensrichtlinien, ohne Bedenken oder Angst vor Vergeltungsmaßnahmen, gemeldet werden können. („*Communication beyond Normal Channels*“) Für Kommunikation gilt immer noch, dass persönliche Gespräche am effektivsten sind, trotz der stark digitalisierten Umwelt, in der ein Unternehmen arbeitet. Dieser persönliche Kommunikationsweg ist in internationalen Unternehmen nur mit hohen Kosten umzusetzen, daher muss mit unterschiedlichen Methoden zur Kommunikation gearbeitet werden, bei welchen verbale und nonverbale, kulturelle, ethnische und Generationsunterschiede sowie der Zeitpunkt und die formalistischen Kommunikationsmerkmale eine große Bedeutung haben. („*Method of Communication*“)[159]

- “*The organization communicates with external parties regarding matters affecting the functioning of internal control.*” [160]

Kommunikation ist nicht nur für interne, sondern auch für externe Informationen von Bedeutung, vor allem bei der Zusammenarbeit mit externen Servicepartnern, welche einen Einfluss auf die unternehmerischen Ziele und internen Control-Ziele haben. Bei der externen Kommunikation gelten dieselben Prinzipien wie bei interner Kommunikation, erweitert um den Faktor, dass gewisse für Unternehmensexterne zugänglich Informationen zu einer Schädigung des Unternehmens und illegalen Handlungen führen können. Eigene Distributionsprozesse und Regulierungen zur Kommunikation mit Externen sollten deshalb Teil der Ziel-, Risiko- und Prozessdefinition sein und in das interne Kontrollsystem integriert werden. („*External Communication*“, „*Communication beyond Normal Channels*“ und „*Method of Communication*“)[161]

4.2.3.5 Monitoring Activities

Die Rahmenbedingungen der Unternehmenstätigkeiten als auch die Kontrolldimensionen verändern sich kontinuierlich, daher muss die Qualität der internen Kontrollen regelmäßig beurteilt und, wo notwendig, angepasst werden. Diese laufende Überwachung erlaubt es, Probleme oder Fehler frühzeitig zu erkennen und schnell korrektive Maßnahmen zu ergreifen. Dem steht eine separate Evaluierung des internen Kontrollsystems als Ganzes, welche meist durch eine interne Revision erfolgt, gegenüber.[162]

---

[159] Vgl. COSO2013, S.113-117.
[160] COSO2013, S.105.
[161] Vgl. COSO2013, S.118ff.
[162] Vgl. Jenal2006, S.28ff.

- „*The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning*.“[163]

Die Überwachung des internen Kontrollsystems durch laufende, gesonderte oder eine Kombination laufender und gesonderter Beurteilung soll sicherstellen, dass die Angemessenheit des Aufbaus und die Funktionsfähigkeit der Kontrollen und des internen Kontrollsystems selbst gegeben sind. Die laufende Beurteilung sollte dabei Teil des internen Kontrollsystems selbst sein und als Teil der kontinuierlichen Managementaufgaben definiert sein. („*Ongoing Evaluations*“) Eine gesonderte Beurteilung wird periodisch durchgeführt und hat das gleiche Ausmaß wie eine laufende Überprüfung, bietet jedoch durch Separierung vom täglichen Geschäft einen anderen Blickwinkel. Zum Einsatz kommt in diesem Kontext geschultes Personal aus einer prozessfremden Umgebung, wie interne Revisoren, abteilungsfremde oder speziell geschulte Mitarbeiter, aber es können auch Vergleiche zu anderen Unternehmen als Beurteilungsgrundlage gezogen werden. Auch eine separate Selbstevaluierung durch den Prozessverantwortlichen kann zu einem besseren internen Kontrollsystem beitragen. („*Separate Evaluation*“)[164]

- “*The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate*.”[165]

Die Ergebnisse des Überwachungsprozesses sollten in die Risikobeurteilung einfließen, einen Anstoß zur Optimierung des internen Kontrollsystems geben und angemessen dokumentiert werden. „*Deficiencies are those matters that represent a potential or real shortcoming in some aspect of the system of internal control that has the potential to adversely affect the ability of the entity to achieve its objectives.*”[166] („*Assess Results*”) Diese Dokumentation kann als Nachweis für die Überwachungstätigkeit und deren Ergebnisse herangezogen werden, dient aber auch als Möglichkeit zur Kommunikation von aufgetretenen Fehlern und erleichtert die Überwachung aller Korrekturmaßnahmen. („*Communicating Internal Control Deficiencies*“ und „*Monitoring Corrective Actions*“) [167]

[163] COSO2013, S.123.
[164] Vgl. im Folgenden Bungartz2011, S.66f. und COSO2013, S. 128ff.
[165] COSO2013, S.123.
[166] COSO2013, S.133.
[167] Vgl. im Folgenden Löffler2011, S.198 und COSO2013, S.133ff.

4.2.4 Grenzen des Internal Control Konzepts

„*Internal control, no matter how well designed, implemented and conducted, can provide only reasonable assurance (…) of the achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all systems of internal control. These include the realities that human judgment in decision making can be faulty, external events outside the organization's control may arise, and breakdowns can occur because of human failures such as making errors. Additionally, controls can be circumvented by two or more people colluding, and because management can override the system of internal control.*"[168]

Interne Kontrollen bieten nur eingeschränkten Schutz gegen Betrug und Unternehmenspleiten. Da dieses auf verschiedenen Ebenen für unterschiedliche Ziele eingesetzt wird, können Ziele in Bezug auf die Effektivität und Effizienz der Geschäftstätigkeit des Unternehmens nicht hinreichend abgesichert werden. Internal Control kann für die Erreichung und Auswirkung von Unternehmenszielen nur eingeschränkte Sicherheit bieten, da die Wirksamkeit des Internen Kontrollsystems vor allem durch menschliche Schwächen eingeschränkt wird:

- Fehleinschätzungen in Geschäftsentscheidungen, welche unter Zeitdruck und mit eingeschränkten Informationen getroffen werden, führen zu Fehlentscheidungen, welche in der Regel erst im Nachhinein festgestellt und korrigiert werden können.
- Führungskräfte, welche sich über bestehende Kontrollvorschriften hinwegsetzen (*Management Override*), um sich persönlich zu bereichern, und dabei eine falsche Darstellung von Unternehmensdaten oder Verschleierung von Gesetzesverstößen bewirken. Dabei ist jedoch zu beachten, dass nicht jeder Eingriff des Managements in das Interne Kontrollsystem als negative oder illegale Handlung qualifiziert werden kann, da in manchen Fällen eine Änderung von bestehenden Vorschriften und damit abweichende Regelungen notwendig sind.
- Absprachen zwischen handelnden Personen, die gemeinsam etwas geheim halten oder verbergen, indem konkrete Informationen zurückgehalten oder geändert werden, um sich selbst oder andere zu bereichern oder zu schützen. Dabei wird die durch die Funktionstrennung erzielte Kontrollwirkung übergangen und eine Aufdeckung durch Internal Control zunichte gemacht.
- Selbst die besten Kontrollinstruktionen können missverstanden werden und mangelnde Sorgfalt, Unachtsamkeit oder Überforderung schränken die Wirksamkeit von theoretisch effektiven Kontrollmaßnahmen ein.

Ein weiterer Aspekt, vor allem in der Prüfung des Internen Kontrollsystems durch die Interne Revision, ist maßgeblich die Einhaltung der wesentlichen Grundsätze, wie das Vier-

[168] COSO20136, S.137.

Augen-Prinzip und die Funktionstrennung sowie der Soll-Ist-Vergleich zwischen dem Vorgegebenen und dessen Einhaltung in den Prozessen. Um einen Soll-Ist-Vergleich durchzuführen, müssen sowohl der Sollzustand als auch der Istzustand vorhanden und bewertbar sein, wobei vor allem der Sollzustand teilweise durch kurzfristig auftauchende Ereignisse, Eigeninitiativen oder risiko- und chancenreiche Herausforderungen, welche im Sollzustand noch keine entsprechenden Themen waren, abweichen kann.

Selbst ein funktionierendes Internal-Control-System kann die Erreichung von Unternehmenszielen nicht garantieren, sondern nur den Fortschritt der Zielerreichung zeigen und gleichzeitig viele Risiken ausschalten oder reduzieren. „*Notwithstanding there inherent limitations, management should be aware of them when selecting, developing, and deploying controls that can, to the extent practical, minimize them.*"[169] [170]

[169] COSO2013, S.138.
[170] Vgl. im Folgenden Klawatsch1995, S.51f.; COSO2013, S.138ff.; Root1998, S.140f. und IIA2004, S.59f.

5 Internal Control – Integrated Framework 1992 und 2013 im Vergleich

Am 14. Mai 2013 wurde das Internal Control – Integrated Framework vom Committee of Sponsoring Organizations of the Treadway Commission in einer neuen Version herausgegeben, um den Änderungen in Unternehmen und dem Unternehmensumfeld Rechnung zu tragen. „*The 2013 Framework retains the definition of internal control and the COSO cube, including the five components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.*"[171] Gleichzeitig enthält die überarbeitete Version Verbesserungen und Klarstellungen, die wichtige Erweiterung der 5 Komponenten des Internal Control um 17 Kernprinzipien, um so eine Erleichterung der Gestaltung und Umsetzung interner Kontrollsysteme zu ermöglichen, die Erweiterung der Zielkategorie Financial Reporting, um die anderen Formen der Berichterstattung mit einzuschließen, und die erweiterte Betrachtung von Betrug und betrügerischen Handlungen im Unternehmen. „*The COSO board has stated that users should transition to the new 2013 framework in their applications and related documentation as soon as possible, given their particular circumstances. The COSO board believes that the key concepts and principles embedded in the original 1992 framework are fundamentally sound and broadly accepted in the marketplace, and it will continue to make the 1992 version available through December 15, 2014, after which it will be considered superseded.*"[172] [173]

[171] KPMG26_2013/05, S.1.
[172] Moeller2014, Chapter 20 (e-book).
[173] Vgl. im Folgenden KPMG26_2013/05, S.1f. und COSO2013, Foreword S.i.

5.1 Begründung für die Neuauflage des Internal Control – Integrated Framework

Das Committee of Sponsoring Organizations of the Treadway Commission hat die Neuauflage des Internal Control – Integrated Framework im November 2010 mit der Begründung, dass „*this initiative is expected to make the existing Framework and related evaluation tools more relevant in the increasingly complex business environment so that organizations worldwide can better design, implement, and assess internal control*"[174], angekündigt. Diese Änderungen wurden vor allem durch die richtungsweisenden Veränderungen, die seit 1992 zu einschneidenden Änderungen der wirtschaftlichen Rahmenbedingungen geführt haben, angestoßen[175]:

- Geschäftsmodelle haben sich wesentlich verändert, die Märkte werden immer weiter globalisiert; und es kommt vermehrt zu grenzüberschreitenden Fusionierungen und Übernahmen von Unternehmen, wodurch eine Anpassung der Strukturen und Betriebsmodelle sowie den jeweiligen Verantwortungen und Zuständigkeiten im Unternehmen und Unternehmenseinheiten notwendig ist. Dieser Umstand hat eine wesentliche Auswirkung auf das interne Kontrollumfeld, die internen und externen Risikofaktoren und die damit zusammenhängenden Verantwortungszuordnung.
- Unternehmen, welche ihr Geschäftsmodell um die Nutzung von Shared Services, Outsourcing-Dienstleistungen erweitert haben, um im gegebenen Wettbewerbsumfeld, mit den technologischen Veränderungen und dem Kostendruck standzuhalten, ist um ein Wesentliches gestiegen. In diesen erweiterten Geschäftsmodellen muss die Verantwortung für die internen Kontrollen festgelegt werden, um ein wirksames internes Kontrollsystem sicherzustellen.
- Beinahe jedes Unternehmen und jede Unternehmenseinheit nutzen heutzutage IT-Systeme und verwandte Technologien, welche „*have evolved from large standalone mainframe environments that process batches of transactions to highly sophisticated, decentralized, and mobile applications involving multiple real - time activities that can cut across many systems, organizations, processes, and technologies*"[176], und haben damit eine signifikante Auswirkung auf die Implementierung und Verwaltung von internen Kontrollverfahren, vor allem im Hinblick auf automatisierte IT-basierte Kontrollen und Prozesse, die diese Kontrollen entwickeln, installieren und überwachen.
- Regeln, Vorschriften und Normen für Unternehmen umfassen durch die starke Veränderung der wirtschaftlichen Rahmenbedingungen eine höhere Komplexität und werden in kürzeren Zeitabschnitten an die Neuerungen in den Unternehmensstrukturen und Geschäftsmodellen angepasst. Dadurch ändern sich Anforderun-

[174] COSO.org11/2010, S1.
[175] Vgl. im Folgenden COSO.org11/2010, S.1; Burger2012, S.95; Moeller2014, Chapter3 (e-book) und COSO.org06/2013, S.2.
[176] COSO2013, S.174.

gen an die externe Berichterstattung, muss regelmäßig überprüft und in den Zielen festgehalten werden, um Kriterien zur Beurteilung von Mängeln festzusetzten.

- Diese Änderungen folgen dem klassischen internen Kontrollansatz nicht, und aufgrund der erhöhten Komplexität erhöhen sich auch die Anforderungen und Erwartungen hinsichtlich Governance Oversight im Zusammenhang mit Risikomanagement, Prüfungen, Vergütungen und Nominierungen.
- Es gibt eine breite Palette von Antikorruptions- und Betrugsbekämpfungs-Vorschriften und Gesetzten, welche vor allem in den letzten Jahren, aufgrund von verschiedenen Betrugsfällen in Unternehmen, Eingang in die Legislative gefunden haben. Dadurch hat sich auch der Zusammenhang zwischen Betrugspotenzial und Internen Kontrollen verstärkt.[177]

„*Each of these changes requires an enterprise to evaluate these implications on its systems of internal control, with an emphasis on its external financial reporting, and to design and implement appropriate responses so that their systems of internal control adapt and remain effective over time*."[178]

Das COSO Framework stellt jedoch selbst nach Anpassung keine Reihe von Standards und Regeln auf, welche umgesetzt werden können und dadurch ein Internal Control System bieten, sondern umfasst weiterhin ein Rahmenwerk welches ein Unternehmen bei der Umsetzung und Kontrolle ihrer Prozesse und Systeme, durch besseres Verständnis von internen Kontrollverfahren, unterstützt. Die wichtigsten Konzepte und Prinzipien „*embedded in the original Framework remain fundamentally sound for designing, implementing, and maintaining systems of internal control and assessing their effectiveness*"[179]. Durch die Anpassung des Frameworks werden die im Original eingebetteten Grundsätze formalisiert; so sind Lücken im existierenden Internal-Control-Rahmen eines Unternehmens leichter aufzudecken und abzudecken.[180]

[177] Vgl. im Folgenden COSO.org11/2010, S.1; Burger2012, S.95; Moeller2014, Chapter3 (e-book); COSO2013, S.173f. und COSO.org06/2013, S.2.
[178] Moeller2014, Chapter 3 (e-book).
[179] COSO.org06/2013, S.2.
[180] Vgl. im Folgenden Moeller2014, Chapter 3 sowie Chapter 20 (e-book) und COSO.org06/2013, S.2f.

5.2 Anpassungen des Integrated Framework 1992 zu 2013

5.2.1 Definition von Internal Control, Objectives und Components

Im original COSO Internal Control – Integrated Framework 1992 wurde Internal Control wie folgt definiert, "*Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

- *Effectiveness and efficiency of operations.*
- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations*."[181]

Diese Definition wurde in der im Jahr 2013 veröffentlichten Anpassung nicht verändert. Ein wesentlicher Unterschied ergibt sich im Vergleich zur ersten Auflage in der Darstellung, da diese Definition anhand einer Pyramide „*with five layers or interconnected components comprising the overall internal control system*"[182] dargestellt wird, welche als Grundlage das sogenannte Kontrollumfeld (*Control Environment*) hat und anschließend in vier horizontale interne Komponenten gegliedert wird, welche von der Komponente *Communication and Information* als Schnittstelle miteinander verbunden werden. „*The **control environment** provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components. Within this environment, management **assesses risks** to the achievement of specified objectives. **Control activities** are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant **information** is captured and **communicated** throughout the organization. The entire process is **monitored** and modified as conditions warrant*."[183] [184]

[181] COSO1994, S.13.
[182] Moeller2014, Chapter 3 (e-book).
[183] COSO1994, S.17.
[184] Vgl. im Folgenden Moeller2014, Chapter 3 (e-book) und COSO1994, S.17ff.

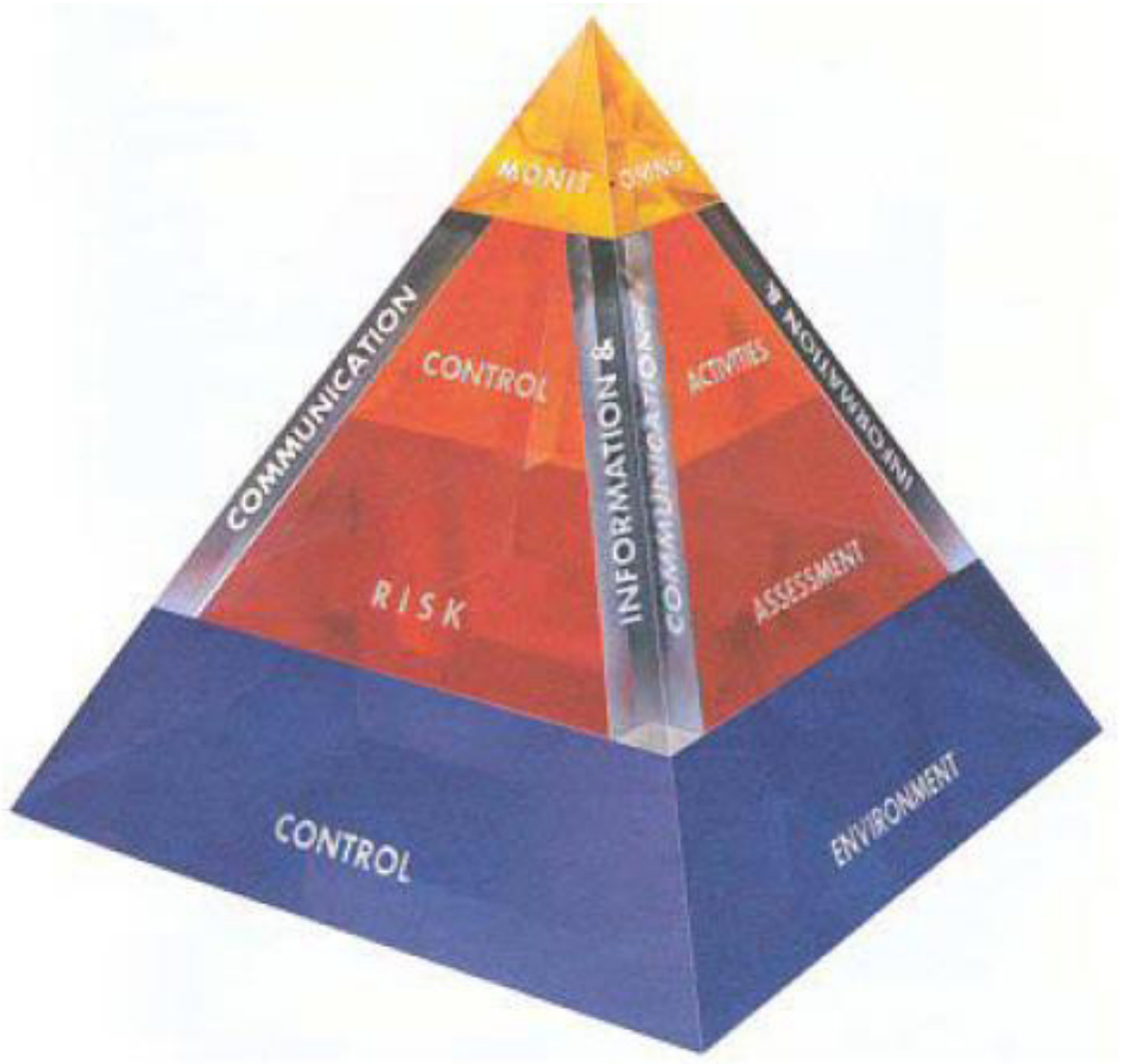

Abb. 11 Internal Control Components[185]

Diese Darstellung wird in der neu überarbeiteten Version von 2013 nicht mehr aufgegriffen, da zusätzlich zu den Komponenten des Internal Control die Wechselbeziehung zu den Kontrollziel-Gruppen und dem gesamten Unternehmen, welches durch den Internal Control Cube dargestellt wird, in den Vordergrund rückt. Diese wird in der Auflage von 1992 erst in der detaillierten Beschreibung der Beziehung zwischen den *Objectives* und *Components* dargestellt, zwar in demselben Kontext, jedoch zur Erreichung von einzelnen Zielen und nicht als Kontrollmechanismus für das gesamte Unternehmen. „*The whole idea of this model is that internal control for today's enterprise is not a single control objective but a multilevel, multifaceted concept, with each unit in the COSO model having a relationship to other components in all three dimensions*."[186] [187]

[185] COSO1994, S.17.
[186] Moeller2014, Chapter 3 (e-book).

Abb. 12 Internal Control Cube Version 1992 im Vergleich zu Version 2013[188]

[187] Vgl. im Folgenden Moeller2014, Chapter 3 (e-book); COSO1994, S.18ff. und COSO2013, S.5ff.
[188] Vgl. im Folgenden COSO1994, S.19 und COSO2013, S.5.

Wie in Abbildung 12 gezeigt wird, waren die Bestandteile des ursprünglichen Rahmens dieselben, und man hat mit der neu beschriebenen, überarbeiteten Version die Abschnitte detaillierter beschrieben, teilweise umbenannt und das Verhältnis der jeweiligen Komponenten zu den Zielen gestärkt. Die frühere Pyramidenstruktur, welche die Components im COSO-Würfel wiedergibt, zeigte das Control Environment als Grundpfeiler für alle internen Kontrollverfahren ohne Bezug auf die Ziele. Um ein ausgeglichenes Internal Control System für ein Unternehmen zu schaffen, ist aber eine ausgeglichene Einhaltung aller Komponenten und deren Prinzipien in Bezug auf das gesamte Unternehmen und deren Ziele von Relevanz, was mit dem überarbeiteten COSO-Würfel besser zur Geltung kommt.[189]

„*The original framework stated that objective setting was a management process, and that establishing objectives is a precondition to internal control*.“[190] Diese Ziele auf Unternehmensebene spiegeln Entscheidungen des Vorstands wider, wie eine Organisation versucht, Wertschöpfung zu generieren, zu bewahren und zu erkennen, und sind damit die Voraussetzung für interne Kontrollen als wichtiger Bestandteil der Managementprozesses in Bezug auf die strategische Planung. „*It is not practical to design and implement a system of internal control unless the entity's objectives and related sub-objectives are parts of or flow from the strategic-planning process, with consideration given laws, rules, regulations, and standards as well as management's own choices. (…) Internal control cannot dictate or establish what an entity's objectives should be*.”[191] Im Rahmen des internen Kontrollsystems eines Unternehmens müssen Ziele messbar und zeitbasiert quantifiziert, die Eignung der Ziele und Teilziele für interne Kontrollen bestimmt und im gesamten Unternehmen kommuniziert werden. Internal Control ist ein dynamischer, integrierter Prozess, und viele Kontrollen sind miteinander verknüpft; und Ziele, die einer Zielkategorie zugeordnet sind, können sich überschneiden oder die Zielerreichung anderer Ziele unterstützen sowie in der Zuordnung variieren, abhängig von Situationen und Verbindungen zu anderen Zielen. Somit betrachtet das überarbeitete Framework die drei Zielkategorien weder als Teil einer Einheit oder des gesamten Unternehmens noch als Teil nur einer Internal-Control-Komponente, sondern in dem Sinne, dass alle Ziele in den drei Zielkategorien und jede Komponente sich überschneiden können und in jeder betroffenen Unternehmenseinheit gelten.[192]

---

[189] Vgl. im Folgenden Moeller2014, Chapter 3 (e-book); KPMG26_2013/05, S.1f.; COSO1994, S.18 und COSO2013, S.175.
[190] COSO2013, S.173.
[191] COSO2013, S.15.
[192] Vgl. im Folgenden COSO2013, S.6f. sowie S.15; Moeller2014, Chapter 3 (e-book) und KPMG26_2013/05, S.2f.

5.2.2 Anpassungen der Zielkategorien des Internal Control und die Erweiterung der Reporting Objectives

Der erste Schritt zur Etablierung von wirksamen internen Kontrollen in einem Unternehmen ist die Einrichtung von Zielen auf Unternehmensebene, die die Entscheidungen des Vorstands widerspiegeln, um Wertschöpfung zu erkennen, zu generieren und zu bewahren. „*Objectives should be established covering the total entity or enterprise, but sublevel or detailed objectives can be built by division or operating units or for specific business units or activities. Each should be built to satisfy the COSO framework's financial reporting, operations, and compliance objectives.*"[193] Diese Zielkategorien wurden bereits im COSO Framework 1992 als relevant beschrieben und haben sich grundsätzlich in der Neuauflage nicht geändert, sondern wurden nur teilweise angepasst und erweitert[194]:

- „***Operations Objectives*** *– related to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss. In the 1992 Framework, the operations objective was limited to "effective and efficient use of the entity's resources."*
- ***Reporting Objectives*** *– related to internal and external financial and nonfinancial reporting to stakeholders, which would encompass reliability, timeliness, transparency, or other terms as established by regulators, standard setters, or the entity's policies. In the 1992 Framework, the reporting objective was called the financial reporting objective and it was described as "relating to the preparation of reliable financial statements."*
- ***Compliance Objectives*** *– related to adhering to laws and regulations that the entity must follow. In the 1992 Framework, the compliance objective was described as "relating to the entity's compliance with applicable laws and regulations." The 2013 Framework considers the increased demands and complexities in laws, regulations, and accounting standards that have occurred since 1992.*""[195]

Die Ursprünge bei der Bewertung der Zielkategorien im Jahr1992 hatten ihre Wurzeln bei Bedenken über ungenaue oder betrügerische externe Finanzberichterstattung, vor allem da Investoren, Aufsichtsbehörden und Führungskräfte auf allen Ebenen erwarten, dass externe Finanzberichte von Unternehmen korrekt, genau und mit effektiven internen Kontrollen vorbereitet werden. Vor allem durch die Nutzung der SEC, um die Wirksamkeit der internen Kontrollen über die Finanzberichterstattung auf jährlicher Basis zu beurteilen, wurde dieser Ansatz gestärkt. Die Finanzberichterstattung ist auch in der neu überarbeiteten Version des Internal Control Framework ein Hauptbestandteil für die Wirksamkeit eines internen Kontrollsystems. „*Whereas the reporting category of objectives was leveraged primarily for external financial reporting in the past, this category now explicitly and*

---

[193] Moeller2014, Chapter 3 (e-book).
[194] Vgl. im Folgenden COSO2013, S.6f. sowie S.15; Moeller2014, Chapter 3 (e-book) und KPMG26_2013/05, S.2f.
[195] KPMG26_2013/05, S.2 und S.3.

more clearly encompasses both internal and external financial and nonfinancial reporting objectives."[196] [197]

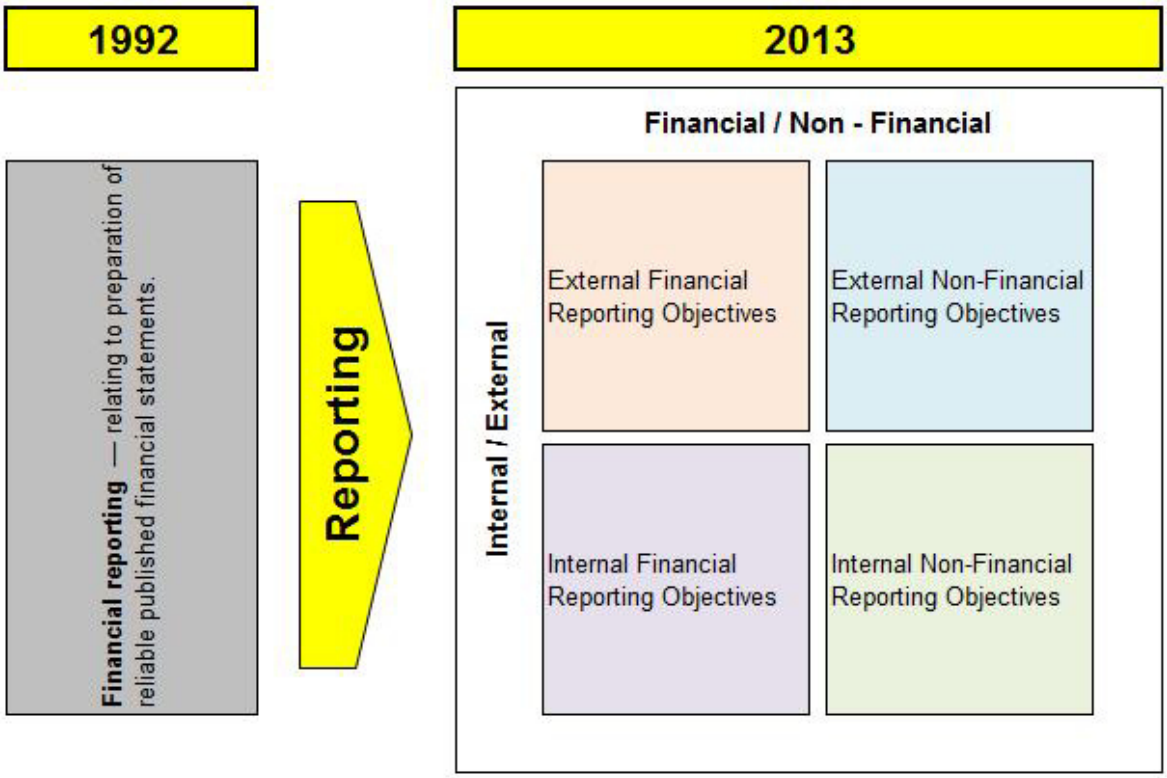

Abb. 13 Vergleich der Reporting Objectives von COSO 1992 zu COSO 2013[198]

In jedem Unternehmen werden beträchtliche Ressourcen für die Entwicklung von finanziellen und nichtfinanziellen Berichten für interne Zwecke genutzt. Diese Berichte unterstützen oder fließen in externe Berichte ein und betreffen Informationen, die regelmäßig für die operativen Geschäftstätigkeiten benötigt werden, die sich auch ohne Relevanz für die externe Finanzberichterstattung auf den Erfolg des Unternehmens auswirken können, da beinahe alle Unternehmensberichte eine finanzielle Auswirkung in der Zeit- und Kostenfrage haben. Daher ist es wichtig, dass alle Berichte mit derselben Relevanz für das Unternehmen und die Internal-Control-Ziele betrachtet werden wie Berichte für externe Finanzberichterstattungen.[199]

[196] COSO.org06/2013, S.4.
[197] Vgl. im Folgenden Moeller2014, Chapter 3 (e-book); COSO2013, S.8f. und KPMG26_2013/05, S.3f.
[198] Vgl. im Folgenden COSO2013, S.9 und COSO1994, S.16.
[199] Vgl. Moeller2014, Chapter 3 (e-book).

5.2.3 Änderungen in den Components von Internal Control und Einführung des Principle based approach

Das COSO Internal Control – Integrated Framework definiert fünf Komponenten des Internal-Control-Konzepts:

- Control Environment
- Risk Assessment
- Control Activities
- Information an Communication
- Monitoring Activities

„*The 1992 Framework conceptually introduced 17 relevant principles associated with the five components of internal control. But these concepts were implicit in the narrative. Because they are essential in assessing that the five components are present and functioning, these concepts are now explicitly articulated in the 17 principles.*"[200] Diese Prinzipien der Internal-Control-Komponenten sollen zu einem besseren Verständnis über wirksame interne Kontrollen beitragen und als Orientierungshilfe das Management bei der Konzeption, Implementierung und Durchführung von internen Steuerungsprozessen und bei der Beurteilung, ob die einschlägigen Grundsätze vorhanden sind und diese funktionieren, behilflich sein. Jedes der 17 Kernprinzipien beschreibt einen Schwerpunkt, ohne jedes Kernprinzip an sich einer separaten Beurteilung zu unterziehen, welche dann einer der fünf Komponenten zugeordnet sind, und bieten damit ein Konzept zum einfacheren Verständnis des COSO Internal Control – Integrated Frameworks. *„The overall assessment of the effectiveness of an enterprise's internal controls is very much tied to its relationship to COSO's five internal control components and the supporting 17 principles."*[201] [202]

[200] COSO.org06/2013, S.4 und 5.
[201] Moeller2014, Chapter3 (e-book).
[202] Vgl. im Folgenden Moeller2014, Chapter 3 (e-book); COSO1994, S.18ff. und COSO2013, S.5ff.

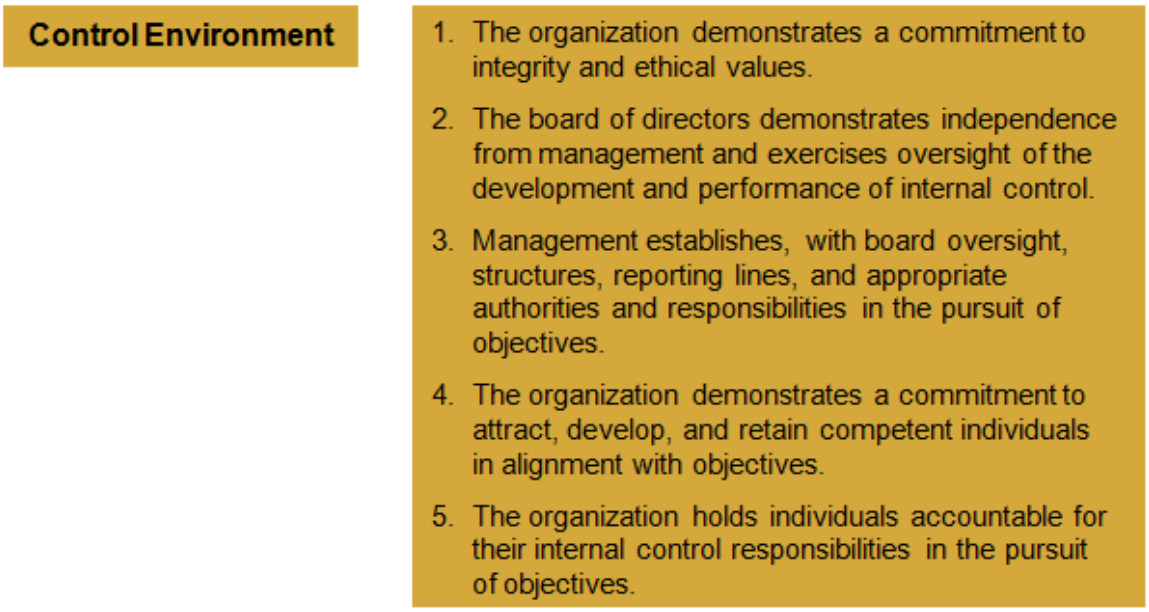

Abb. 14 Kernprinzipien der Internal Control Komponente *Control Environment*[203]

Die ursprüngliche Version des Internal Control Frameworks beschreibt und zeigt im COSO Würfel die Komponente Control Environment als Basis der internen Steuerungskomponenten. Ohne dabei eine begriffliche Änderung vorzunehmen, wird in der neuen Version das Kontrollumfeld an die oberste Stelle gesetzt, da es weiterhin die Grundlage für ein funktionierendes internes Kontrollsystem darstellt und mit der neuen Platzierung ein erhöhtes Maß an Bedeutung zugewiesen wird. Dieser Umstand ist vor allem zurückzuführen auf den „*increased need for transparency of how the organization operates and governs itself; reporting now extends beyond financial performance; risk discussions are expected to be more robust and detailed; corporate social responsibility reporting matters more to stakeholders; and the pace for publishing such information has accelerated*."[204] Das Kontrollumfeld wird von internen und externen Faktoren beeinflusst und muss durch Standards, Verfahren und Strukturen definiert werden, um in den verschiedenen Unternehmensebenen eine Wahrnehmung für interne Kontrollen zu schaffen und bei der Verfolgung der Ziele des Unternehmen ein wirksames Kontrollumfeld sicherzustellen. Während die sieben wichtigsten Faktoren des Control Environment im 1992 Framework, "*integrity and ethical values; commitment to competence; board of directors or audit committee; management's philosophy and operating style; organizational structure; assignment of authority and responsibility; and human resource policies*"[205], zusammengefasst sind, werden nach dem *Principle based approach* im 2013 Framework fünf Kernprinzipien definiert, die verschiedene Komponenten von Internal Control miteinander ver-

[203] Vgl. COSO2013, S.31.
[204] COSO2013, S.175.
[205] KPMG26_2013/05, S.4.

binden, und damit aufgezeigt, dass das Control Environment die Grundlage für ein solides interne Kontrollsystem darstellt. Neben dieser grundlegenden Erweiterung der Definition des Kontrollumfelds sind die folgenden Änderungen ausschlaggebend[206]:

- *„Expanding the discussion of governance roles in an organization, recognizing differences in structures, requirements, and challenges across different jurisdictions, sectors, and types of entities.*
- *Clarifying the expectations of integrity and ethical values to reflect lessons learned and developments in ethical and compliance (e.g. codes of conduct, the attestation process, whistle-blower processes, investigation and resolution, and training and reinforcement both internally and with third parties)*
- *Expanding the notion of risk oversight and strengthening the linkages between risk and performance to help allocate resources to support internal control in the achievement of the entity's objectives*
- *Emphasizing the need to consider internal control across the complexities in organizational structure resulting from different business models and the use of outsourced service providers, business partners, and other external partners.*
- *Aligning roles and responsibilities discussed in organizational structure with the information presented in Appendix B, Roles and Responsibilities, so that major roles are used consistently within the Framework.*"[207]

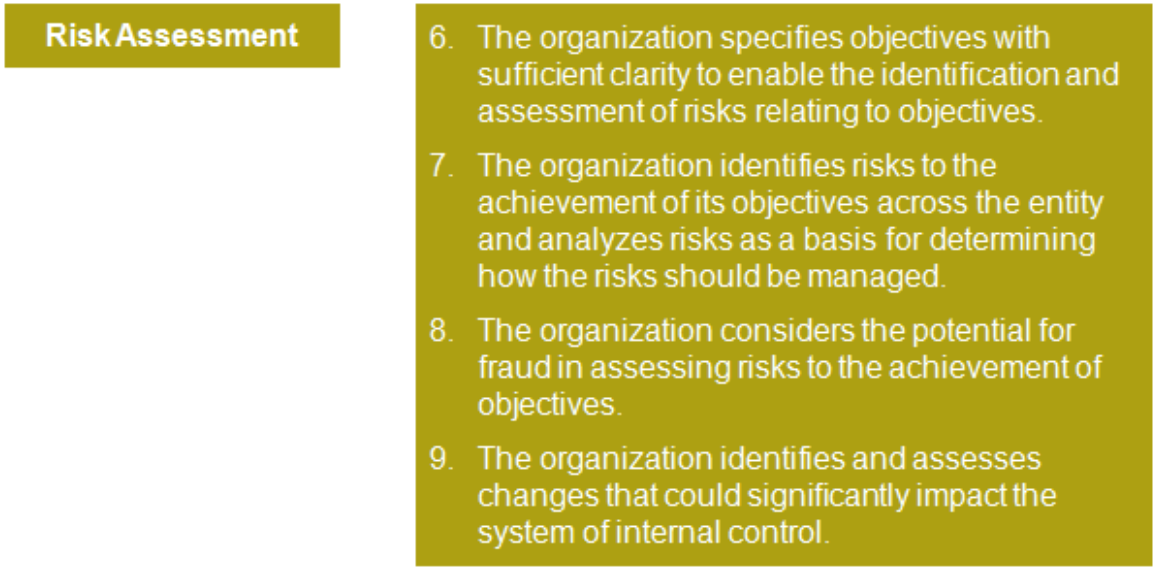

Abb. 15 Kernprinzipien der Internal Control Komponente *Risk Assessment*[208]

[206] Vgl. im Folgenden Moeller2014, Chapter 4 (e-book); COSO2013, S.175f. sowie S.31ff. und KPMG26_2013/05, S.4f.
[207] COSO2013, S.176.
[208] Vgl. COSO2013, S.59.

Jedes Unternehmen ist mit einer Vielzahl von Ereignissen, die die Erreichung von Zielen beeinträchtigen, aus internen und externen Quellen konfrontiert, und Risk Assessment ist dabei ein interaktiver Prozess zur Ermittlung und Bewertung solcher Risiken und Chancen. Diese können die Fähigkeit eines Unternehmens, erfolgreich zu sein, beeinflussen und wurden, nach der ursprünglichen Auflage des COSO Internal Control Integrated Frameworks, in einem sehr ähnlichen, aber mit anderem Hintergrund versehenen Framework zum Enterprise Risk Management aufgenommen. Die interne Kontrollkomponente Risk Assessment fokussiert sich in der Version von 1992 auf drei Bereiche „*management's process for objective setting at an entity-wide and activity level; risk analysis; and managing change*"[209], welche das Hauptaugenmerk auf den Zielen eines Unternehmens haben und dadurch dem Verständnis von Risiken und deren Verknüpfung mit dem Gesamtsystem für interne Kontrollen zur Risikobeurteilung nicht vollständig gerecht werden. Die Änderungen in der COSO 2013 Version werden durch die vier Kernprinzipien verdeutlicht, obwohl die Risikobewertung mit Fokus auf die Zielsetzung im Prinzip 6 Eingang findet und damit weiterhin eine wichtige Voraussetzung für das Risk Assessment ist, das die Aufmerksamkeit um Risiken und dessen Bewertung stärker zu einem risikobasierten Ansatz zu internen Kontrollen führt. In diesem Zusammenhang wurde die Internal-Control-Komponente Risk Assessment um einige Änderungen erweitert[210]:

- „*Focusing the Risk Assessment component on articulating objectives relating to operations, reporting, and compliance with sufficient clarity so that any risks to those objectives can be identified and assessed, and considering the need to assess the suitability of objectives for use as a basis for assessing effectiveness*
- *Broadening the financial reporting category of objectives to include other aspects of external reporting and to include internal reporting*
- *Reflecting the view that non-financial reporting is conducted in relation to an external requirement standard*
- *Clarifying that risk assessment includes processes for risk identification, risk analysis, and risk response*
- *Expanding the discussion on the risk severity beyond impact and likelihood to include velocity and persistence*
- *Incorporating risk tolerances (set as a precondition to internal control and pertaining to the level of acceptable variation in performance and the relative importance of objectives) into the assessment of acceptable risk levels*
- *Expanding the discussion on management needing to understand significant changes in its internal and external factors and how those might impact the overall system of internal control*

[209] KPMG26_2013/05, S.5.
[210] Vgl. im Folgenden COSO2013, S. 176f.; Moeller2014, Chapter 5 (e-book) und KPMG26_2013/05, S.5.

- *Considering fraud risk relating to material omission or misstatement of reporting, inadequate safeguarding of assets, and corruption as part of the risk assessment process*"[211]

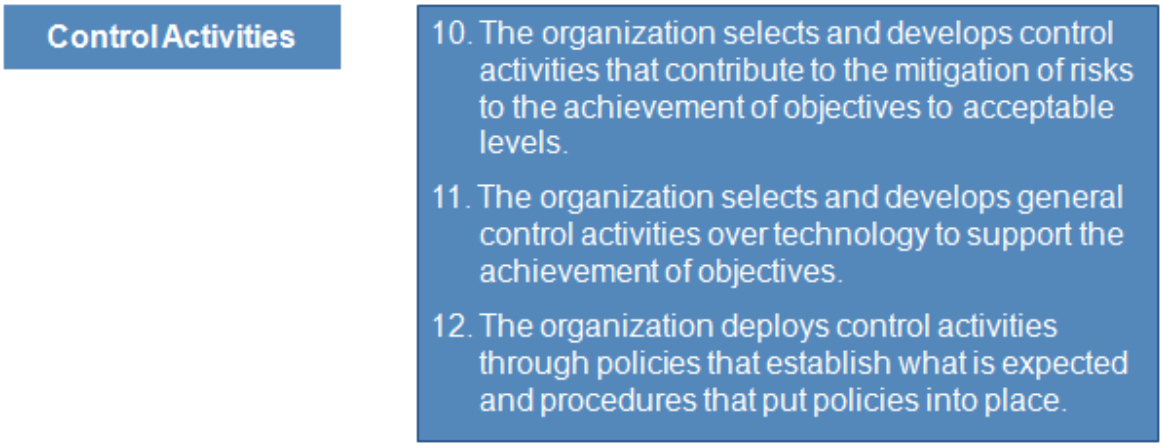

Abb. 16 Kernprinzipien der Internal Control Komponente *Control Activities*[212]

Die Grundsätze der Internal-Control-Komponente Control Activities haben sich seit der Erstauflage des COSO Internal Control – Integrated Frameworks nicht verändert und spiegeln sich auch in den drei Kernprinzipien wider; der Einfluss und die Rolle von Technologie in der Wirtschaft hat jedoch eine starke Auswirkung auf jegliche Kontrollaktivitäten. Es kann festgehalten werden, dass Informationstechnologie heutzutage in die Geschäftsprozesse des gesamten Unternehmens integriert ist und die Vielfalt an Technologien, die einzelne Einheiten verwenden, weitgehend nicht mehr als getrennte Geschäftsbereiche fungieren. Die wichtigste Änderung in dieser Komponente im Vergleich von 1992 zu 2013 betrifft demnach die Technologie und deren Einfluss auf Kontrollaktivitäten, die sich im Detail in den folgenden Punkten auswirken[213]:

- „*Expanding the discussion of the relationship between automated control activities and general controls over technology to reinforce the linkages to business processes, with the details on automated control activities and general controls over technology separated into discrete sections to clarify the distinction between the two*
- *Expanding the discussion that control activities constitute a range of control techniques while providing a more detailed description of these types and techniques, and a way to categorize them; making distinct transaction-level controls from con-*

[211] COSO2013, S.177.
[212] Vgl. COSO2013, S.87.
[213] Vgl. im Folgenden Moeller2014, Chapter 6 (e-book); COSO2013, S.178 und KPMG26_2013/05, S.6.

trols at other levels of the organization; and discussing in more detail information-processing objectives

- *Updating the discussion on general technology controls to focus more on the universal concepts of that needs to be controlled in this area rather than specifics applicable to 1992 technology*"[214]

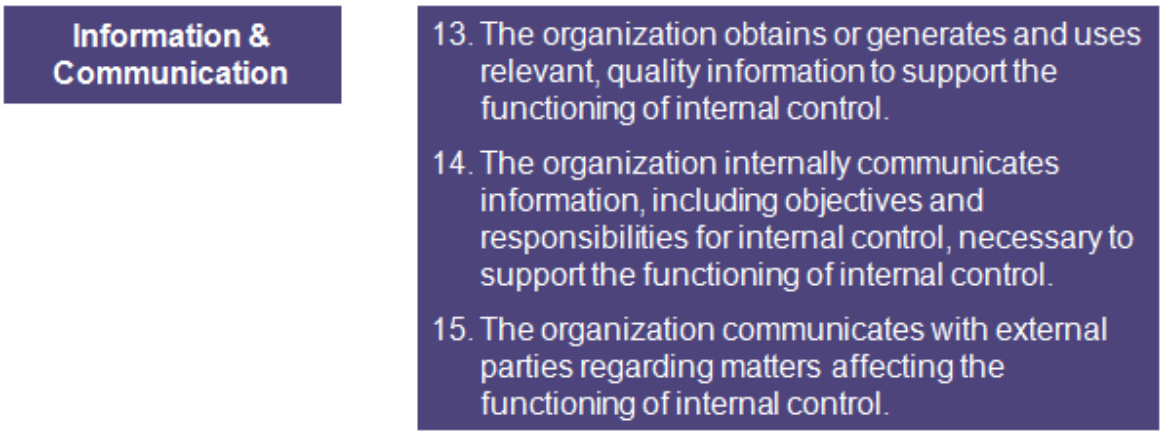

Abb. 17 Kernprinzipien der Internal Control Komponente *Information and Communication*[215]

COSO 1992 zeigt diese Internal-Control-Komponente visuell entlang der Kante eines ansonsten integrierten Rahmens, in der als Pyramidenstruktur beschriebenen Darstellung. Dieser Ansatz hat sich seither dramatisch erweitert, da Informationsquellen vielfältiger und komplexer geworden sind, „*spanning outsourced service providers that support all or part of an organization's business processes (e.g., outsourcing service providers, joint ventures) and internal and extern networks designed to create unstructured information-sharing mechanisms (social media)*"[216], und Kommunikation, wie auch in COSO 2013 genauer definiert, einen kontinuierlichen Prozess zur Bereitstellung, zum Austausch und zur Beschaffung notwendiger Informationen darstellt. Die Menge und Form an zugänglichen Informationen stellt ein Risiko- und Chancenpotential dar, wobei die Bedeutung der Tatsache, die richtigen Informationen zum richtigen Zeitpunkt zur Verfügung zu haben, ein Schlüsselfaktor für erfolgreiche Unternehmenstätigkeiten ist. Durch die Anpassung des Internal Control Frameworks und Erweiterung durch die drei Kernprinzipien dieser Komponente wird eine Guidance zur Einrichtung effizienter Kommunikationsprozesse sowie effektiver Informationsverteilungstechniken geboten[217]:

- „*Emphasizing the discussion of importance of quality of information*

[214] COSO2014, S.178.
[215] Vgl. COSO2013, S.105.
[216] COSO2013, S.178.
[217] Vgl. im Folgenden Moeller2014, Chapter 7 (e-book); COSO2013, S.178f. und KPMG26_2013/05, S.7.

- *Expanding the discussion of the expectations for verifying to a source and for retention when information is used to support reporting objectives to external parties*
- *Expanding the discussion on the impact of regulatory requirements on reliability and protection of information*
- *Expanding the discussion on the volume and sources of information in light of increased complexity of business processes, greater interaction with external parties, and technology advances*
- *Reflecting the impact of technology and other communication mechanisms on the speed, means, and quality of the flow of information*
- *Adding content on the information and communication needs between the entity and third parties, emphasizing the importance of considering how processes may occur outside the entity (e.g., by the use of third-party service providers that manage specific processes) and how the entity needs to obtain information from and communicate with parties that operate outside its legal and operational boundaries*"[218]

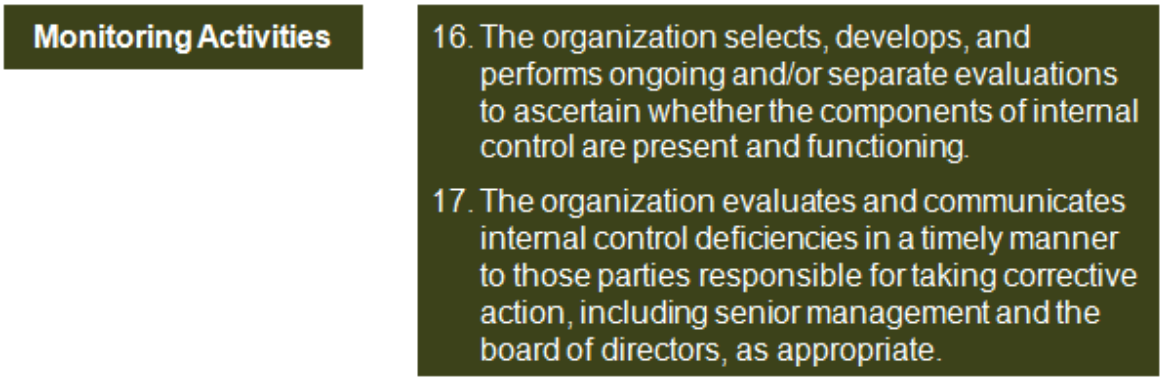

Abb. 18 Kernprinzipien der Internal-Control-Komponente *Monitoring Activities*[219]

Die Internal-Control-Komponente Monitoring wurde in der neu überarbeiteten Auflage des COSO Frameworks nicht nur umbenannt in Monitoring Activities, auch die visuelle Positionierung wurde von der Spitze der Pyramiden-Darstellung auf die Basis, unter den anderen Komponenten, des COSO Würfels verschoben. Trotz der Neupositionierung und Umbenennung wird die Monitoring-Komponente als Schlüsselelement in der internen Kontrolllandschaft verstanden und muss sichergestellt werden, um die internen Kontrollprozesse effektiv zu betreiben. „*When monitoring is designed and implemented appropriately, an enterprise will benefit from these monitoring processes because it is more likely to*

[218] COSO2013, S.179.
[219] Vgl. COSO2013, S.123.

- *Identify and correct internal control problems on a timely basis.*
- *Produce more accurate and reliable information for use in decision making.*
- *Prepare accurate and timely financial statements.*
- *Be in a position to provide periodic certifications or assertions on the effectiveness of internal controls.*"[220]

In der ursprünglichen Version wurden Monitoring Acitivites in erster Linie als Teil der internen Revision oder übergeordneter Management-Überwachungs-Verfahren beschrieben, für ein effektives internes Kontrollsystem ist aber eine laufende Evaluierung durchzuführen, um Mängel zu identifizieren, im gesamten COSO Kontrollumfeld zu kommunizieren und zu beheben. „*However, a management review control that is a monitoring activity would ask why the errors exist, and then assign the responsibility of fixing the process to the appropriate personnel. A monitoring activity assesses whether the controls in each of the five components are operating as intended.*"[221] Demnach wurde die COSO-2013-Komponente Monitoring Activities um folgende Schwerpunkte ergänzt[222]:

- „*Refining the terminology, where the two main categories of monitoring activities are now referred to as "ongoing evaluations" and "separate evaluations"*
- *Adding the need for a baseline understanding in establishing and evaluating ongoing and separate evaluations*
- *Expanding discussion of the use of technology and external service providers*"[223]

[220] Moeller2014, Chapter 8 (e-book).
[221] KPMG26_2013/05, S.7 und 8.
[222] Vgl. im Folgenden Moeller2014, Chapter 8 (e-book); COSO2013, S.179f. und KPMG26_2013/05, S.7f.
[223] COSO2013, S.179 sowie 180.

5.2.4 Definierte Anforderungen für effektive Internal Control

Ein effektives internes Kontrollsystem bietet angemessene Sicherheit zur Zielerreichung eines Unternehmens, dabei ist es sowohl für das Unternehmen als auch die Unternehmenseinheiten relevant und reduziert das Risiko, Ziele der Internal-Control-Zielkategorien nicht zu erreichen. Dazu erfordert ein Internes Kontrollsystem, dass jede der fünf Internal-Control-Komponenten und deren Kernprinzipien vorhanden und funktionsfähig sind:

- *„"Present" refers to the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specific objectives.*
- *"Functioning" refers to the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives."*[224]

Und das die „*five components are operating together in an integrate manner*"[225], da die Komponenten voneinander abhängig sind und die Kernprinzipien innerhalb und zwischen den jeweiligen Komponenten interagieren. „*"Operating together" refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective*"[226] und ermöglichen damit dem Management, eine Entscheidung darüber zu treffen, ob Internal Control im Unternehmen oder der entsprechenden Unternehmenseinheit effektiv ist. Obwohl COSO 2013 jede Komponente und die darin enthaltenen Kernprinzipien als relevant für ein wirksames internes Kontrollsystem impliziert, erfordert es keine separate Auswertung und zeigt einen Entscheidungsspielraum bei der Bestimmung und Eignung oder Relevanz dieser Schwerpunkte. Damit können in Unternehmen, welche in speziellen Industrien tätig sind oder einer spezifischen regulatorischen Situation gegenüberstehen, Prinzipien vom Management ausgeschlossen, ersetzt oder hinzugefügt werden, um die betroffene Komponente und deren Sicherstellung zu gewährleisten.[227]

Bei der laufenden internen Beurteilung und Bewertung der einzelnen Kontrollanforderungen, um festzustellen ob diese vorhanden, funktionsfähig und wirksam sind, oder durch externe Überprüfungen der Kontrollanforderungen kann es zur Aufdeckung von Internal Control Deficiencies kommen, die die Wahrscheinlichkeit des Unternehmens, die Ziele zu erreichen, reduzieren. Diese beziehen sich auf einzelne Mängel in den Kernprinzipien oder Komponenten von Internal Control, welche bewertet, kommuniziert und mit angemessenen Maßnahmen korrigiert werden müssen. Sollte das Management zu dem Schluss kommen, dass eine Komponente und eine oder mehrere Kernprinzipien des Internal Control nicht vorhanden und funktionsfähig sind oder dass die Komponenten

---

[224] COSO2013, S.19.
[225] COSO2013, S.18.
[226] COSO2013, S.19.
[227] Vgl. im Folgenden COSO2013, S.18ff. und Moeller2014, Chapter 3 (e-book).

nicht zusammenarbeiten, wird von einer Major Deficiency gesprochen, die darauf schließen lässt, dass auch keine andere Komponente und kein anderes Kernprinzip das Risiko auf ein akzeptables Niveau abschwächt und damit die Wahrscheinlichkeit, dass ein Unternehmen seine Ziele erreichen kann, stark reduziert. „*Management exercises judgment to assess the severity of an internal control deficiency, or combination of deficiencies, in determining whether components and relevant principles are present and functioning, and components are operating together, and ultimately in determining the effectiveness of the entity's system of internal control.*"[228] Diese Beurteilung ist abhängig von den Unternehmenszielen und wird in einigen Fällen durch die Gesetzgebung und andere relevante Dritte, welche die Kriterien zur Definition von Schwere, Bewertung und Berichterstattung von internen Kontrollmängeln festsetzen, beeinflusst. „*In those instances where an entity is applying a law, rule, regulation, or external standard, management should use only the relevant criteria contained in those documents to classify the severity of internal control deficiencies, rather than relying on the classifications set forth in the Framework*"[229].[230]

5.2.5 Erweiterte Berücksichtigung der Anti-Fraud-Erwartungen

Der US Foreign Corrupt Practices Act (FCPA) war ein frühes Beispiel für die Gesetzgebung für interne Kontrollen und gesetzliche Bestimmungen zur Antikorruptions- und Betrugsbekämpfung aufgrund von sozialen und politischen Unruhen in den 1970er Jahren. Zum ersten Mal wurde das Management eines Unternehmens für angemessene interne Rechnungsprüfung verantwortlich gemacht und damit detaillierte Aufzeichnung über die Konten, Transaktionen und Vermögensgegenstände des Unternehmens zu führen, da bereits damals Betrugsfälle auf einen Mangel an internen Kontrollen zurückzuführen waren. Bei der Veröffentlichung der Auflage von 1992 des COSO Internal Control – Integrated Framework, wurde von den meisten internen und externen Prüfern die Beurteilung und Erkennung von Betrug und betrügerischem Verhalten nicht als wesentlich eingestuft, da dieses vor allem in der Verantwortung von Justizbehörden und Wirtschaftsprüfern ist. Es gibt auch keine direkten Veränderungen zum Thema Betrug in der Neuauflage des COSO 2013 Internal Control – Integrated Frameworks, allerdings enthält die revidierte Auflage eine Anleitung in Form eines Kernprinzips, „*the organization considers the potential for fraud in assessing risks to the achievement of objectives*"[231], der Internal Control Komponente Risk Assessment, die dabei unterstützen soll, das Risiko in Bezug auf das Betrugspotenzial in einem Unternehmen zu bewerten, aufzudecken, und damit die Fähigkeit eines Unternehmens, seine Ziele zu erreichen, beeinflusst. „*Assessment of this prin-*

[228] COSO2013, S.21.
[229] COSO2013, S.21.
[230] Vgl. im Folgenden COSO2013, S.20f.; Moeller2014, Chapter 3 sowie Chapter 8 (e-book) und KPMG26_2013/05, S.8f.
[231] COSO2013, S.78.

ciple may require additional attention by organizations that did not focus their assessment of fraud risk at the specific financial statement account, transaction, or assertion level."[232] Damit sollte einem Risiko, das potenziell betrügerische Situationen betrifft, mehr Aufmerksamkeit zur Absicherung zukommen und bei Erkennung eines dieser Risiken eine Sanierung im Unternehmen eingeleitet werden, da vor allem die Wahrscheinlichkeit von betrugsspezifischen Risiken innerhalb anderer Komponenten des Internal Control und durch Änderungen an den operativen Einheiten des Unternehmen und der Geschäftsprozesse eingedämmt werden kann.[233] „*As part of its risk assessment process, an enterprise should identify the various ways that fraudulent reporting can occur, considering:*

- *The degree of estimates and judgments in external reporting,*
- *Fraud schemes or scenarios common to the industry or markets where the enterprise operates,*
- *History or logistics issues in the geographic regions where the enterprise does business,*
- *Incentives of all types that may motivate fraudulent behavior,*
- *Automation and system-related issues, including weak security and integrity controls,*
- *Vulnerability of management override and potential schemes to circumvent existing internal control activities.*"[234]

[232] KPMG26_2013/05, S.5.
[233] Vgl. im Folgenden COSO2013, S.82 und Moeller2014, Chapter 2, Chapter 3 sowie Chapter 5 (e-book).
[234] Moeller2014, Chapter 5 (e-book)

6 Schlussbetrachtung

„*A system of internal control allows management to stay focused on the organization's pursuit of its operations and financial performance goals, while operating within the confines of relevant laws and minimizing surprises along the way. Internal Control enables an organization to deal more effectively with changing economic and competitive environments, leadership, priorities, and evolving business models*."[235]

Internal Control scheint ein allumfassender Prozess zu sein, welcher einen breiten Ansatz weit über die Finanzberichte und die Aufgaben der Geschäftsführung hinaus umfasst, da die Ziele der Berichterstattung um die Einhaltung, Effizienz und Effektivität ergänzt sind und es damit in den meisten Geschäftstätigkeiten des Unternehmens eingebettete Aktivitäten betrifft. Internal Control ist an die Strategieformulierung und den Ausführungsprozess des Managements gebunden und wird als Form der Risikobehandlung angesehen, da sich die Entwicklung und die Anwendung von Kontrollen als inhärentes Risiko darstellen. Darüber hinaus wird es als eine regulatorische Aufgabe durch Gesetzgebung und Aufsichtsbehörden in der Ausgestaltung und operativen Umsetzung formuliert und teilweise zu einer Offenlegung der internen Kontrollen verpflichtet.[236]

Mehr als ein Jahrhundert der Debatte über die interne Kontrolle zeigt die Bedeutung und die Komplexität des Konzepts, obwohl diese für die meisten nicht außerhalb der Rechnungslegung stattgefunden hat und damit hauptsächlich der direkte Einfluss der internen Kontrollen auf die Finanzberichterstattung in Betracht gezogen wurde. Dabei ist Internal Control ein entscheidender Bestandteil aller Unternehmenseinheiten und beeinflusst den gesamten Corporate-Governance-Mechanismus. Die Fähigkeit eines Unternehmens, Risiken zu managen, hat eine fundamentale Bedeutung in der Unterstützung zur Erreichung von Unternehmenszielen und damit in der Erstellung und Verbesserung von Stakeholder Value. [237]

Neben anderen Ansätzen zum Internal Control wurde vor allem nach der Einführung der PCAOB in den Vereinigten Staaten von Amerika durch den Sarbanes-Oxley Act im Jahr 2002 mit der direkten Reverenz zum COSO Internal Control – Integrated Framework ein breiterer Ansatz für Internal Control eingeführt, welcher nun weltweit als einer der führenden Ansätze für die Unternehmensführung gilt. Dabei stellt das Internal Control Framework keine Reihe an Regeln und Standards zur Einhaltung und Einführung eines internen

[235] COSO2013, S.1.
[236] Vgl. Arwinge2013, S.147f.
[237] Vgl. im Folgenden Arwinge2013, S.148ff. und Moeller2014, Chapter 1 sowie Chapter 20 (e-book)

Kontrollsystems zur Verfügung, sondern lediglich ein Rahmenmodell für den Aufbau eines effizienten Internal-Control-Systems und Prozesses für die berufliche Praxis. [238]

Ein Schlüsselmerkmal des COSO Frameworks ist es, dass nicht nur die Berichterstattung durch die Ziele gedeckt ist, sondern auch Compliance und die Effizienz und Effektivität im Unternehmen, welche messbar und zeitbasiert quantifiziert, die Eignung der Ziele und Teilziele für interne Kontrollen bestimmt und im gesamten Unternehmen kommuniziert werden müssen. Diese Ziele haben Einfluss auf das gesamte Unternehmen und alle Komponenten eines internen Kontrollsystems, die nach COSO in das *Control Environment, Risk Assessment, Control Activities, Information and Communication* und *Monitoring Activities* aufgeteilt sind. Das Internal Control – Integrated Framework hat großen Einfluss auf das Verständnis von Internal Control; und aufgrund der Änderungen in Unternehmen und dem Unternehmensumfeld in den letzten Jahren wurde im Jahr 2013 eine neue Version herausgegeben und damit einige Änderungen eingeführt, um Unternehmen besser bei der Umsetzung von Internal Control zu unterstützen.[239]

Das COSO Framework in seiner ersten Version war nicht sehr detailliert beschrieben und vor allem hat die Einschränkung der Reporting-Ziele auf die Finanzberichterstattung den übergeordneten Ansatz von Internal Control beeinflusst. Obwohl das Konzept von Internal Control und die in der neuen Version vorgestellten Kernprinzipien der Internal Control Komponenten, welche die vielleicht wichtigste Änderung darstellen, impliziert enthalten waren, formuliert das revidierte Rahmenwerk jede Anforderung an die jeweilige Komponente anhand der Kernprinzipien. Bei der Beurteilung durch das Management und zur Sicherstellung eines effektiven internen Kontrollsystems müssen alle fünf Komponenten und deren Kernprinzipien vorhanden und funktionsfähig sein und zusammenarbeiten. Einen wesentlichen Einfluss auf Internal Control hat auch die erhöhte Aufmerksamkeit bezüglich der Risiken in Bezug auf das Betrugspotenzial in Unternehmen und die Unterstützung bei deren Bewertung und Aufdeckung.[240]

Unternehmen sind anhand dieser Änderungen vor die Aufgabe gestellt, den Status und die Schwachstellen ihres internen Kontrollsystems zu überprüfen, selbst wenn diese möglichen Schwachstellen nicht die externe Finanzberichterstattung betreffen, um interne Kontrollen zu stärken und Korrekturmaßnahmen zu ergreifen. Es kann davon ausgegangen werden, dass Internal Control weiterhin eine wichtige Rolle in jedem Unternehmen spielt und damit ein vorhandenes, effektives und starkes Internal Control von großer Bedeutung für jedes Unternehmen ist.[241]

---

[238] Vgl. im Folgenden Arwinge2013, S.147ff. und Moeller2014, Chapter 1 sowie Chapter 20 (e-book)
[239] Vgl. im Folgenden Arwinge2013, S.147ff.; Moeller2014, Chapter 1 sowie Chapter 20 (e-book) und COSO2013, S.5ff.
[240] Vgl. im Folgenden Moeller2014, Chapter 20 (e-book) und COSO2013, S.173ff.
[241] Vgl. Moeller2014, Chapter 20 (e-book).

Literaturverzeichnis

A.C.2009	A.C., Fernando: Corporate Governance: Principles, Policies and Practices, Delhi, Dorling Kindersley (India) Pvt. Ltd., 2009
Arwinge2013	Arwinge, Olof: Internal Control: A Study of Concept and Themes, Heidelberg, Physica-Verlag, 2013
Bloomfield2013	Bloomfield, Stephan: Theory and Practice of Corporate Governance: An Integrated Approach, Cambridge [u.a.], Cambridge Univ. Press, 2013
Brünger2009	Brünger, Christian: Erfolgreiches Risikomanagement mit COSO ERM; Empfehlungen für die Gestaltung und Umsetzung in der Praxis, Berlin, Erich Schmidt, 2009
Bungartz2011	Bungartz, Oliver: Handbuch interne Kontrollsysteme (IKS): Steuerung und Überwachung von Unternehmen, Berlin, Erich Schmidt, 2011
Burger2012	Burger, Anton: Internal Control für Führungskräfte, München, Oldenbourg, 2012
Clarke2012	Clarke, Thomas: The SAGE Handbook of Corporate Governance, London [u.a.], SAGE Publ., 2012
COBIT5_2012	Information Systems Audit and Control Association: COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT, Illinois, ISACA, 2012
COSO1994	Committee of Sponsoring Organizations of the Treadway Commission: Internal Control — Integrated Framework May 1994, n.b., 1994

COSO2013	Committee of Sponsoring Organizations of the Treadway Commission: Internal Control — Integrated Framework March 2013, n.b., 2013
Euler1992	Euler, Karl August: Interne Kontrollen im Unternehmen: Konzepte zur Vermögenssicherung und Effizienzsteigerung, Berlin, Schmidt, 1992
Freidank2008	Freidank, Carl-Christian: Corporate Governance und Interne Revision Handbuch für die Neuausrichtung des Internal Auditings, Berlin, Erich Schmidt, 2008
Füss2005	Füss, Roland: Die Interne Revision - Bestandsaufnahme und Entwicklungsperspektiven, Berlin, Erich Schmidt, 2005
Giller2008	Giller, Barbara: Implementation of the Sarbanes-Oxley Act Section 404 on the basis of standard reference processes, business process (re-)engineering and risk and control measures: a stochastic simulation model, Wien, Hochschulschriften: Wien, Wirtschaftsuniv. Diss., 2008
Helfer2010	Helfer, Michael [Hrsg.]; Bolte, Dirk: Interne Kontrollsysteme in Banken und Sparkassen: Vorgaben und Erwartungen der Bankenaufsicht, Schlüsselkontrollen, IKS-Dokumentationen für die Fachbereiche, IKS-Prüfungen durch interne Revision, Wirtschaftsprüfung und Aufsicht, Heidelberg, Finanz-Colloquium Heidelberg, 2010
Holt2006	Holt, Michael F.: The Sarbanes-Oxley act - overview and implementation procedures manual, Oxford [u.a.], Elsevier, CIMA Publ., 2006
Horvath2003	Horvath, Peter: Vahlens großes Controllinglexikon, München, Beck, 2003
Horvath2012	Horvath, Peter: Controlling, 12.Auflage, Stuttgart, Vahlen, 2012

Huska1996	Huska, Harald: Das Interne Kontrollsystem - Perspektiven der prozeßgebundenen Überwachung, Wien, Wien, Wirtschaftsuniv., Dipl.-Arb., 1998, 1996
IIA2004	Institut für Interne Revision Österreich, Wien: Das Interne Kontrollsystem aus der Sicht der Internen Revision, Wien, Linde, 2004
IIA2006	Institut für Interne Revision Österreich, Wien: Das Risikomanagement aus Sicht der Internen Revision, Wien, Linde, 2006
IIA2008	Institut für Interne Revision Österreich, Wien: Interne Revision - Gestaltung und Organisation in der Praxis, Wien, Linde, 2008
Jenal2006	Jenal, Ladina: Internal Control - Theoretisches und Empirisches zum ganzheitlichen Zusammenwirken der Control-Funktionen, St. Gallen, Hochschulschriften: St. Gallen, Univ. Diss., 2006
Klawatsch1995	Klawatsch, Hans-Peter: Internal Control - Integrated Framework das interne Kontrollsystem (IKS) und seine Bedeutung für den Abschlussprüfer, Wien, Wirtschaftsuniv., Dipl.-Arb., 1996, 1995
Klinger2011	Klinger, Michael A.: ABC der Gestaltung und Prüfung des Internen Kontrollsystems (IKS) im Unternehmen, Wien, Linde, 2011
Knapp2005	Knapp, Eckhard: Interne Revision und Corporate Governance - Aufgaben und Entwicklungen für die Überwachung, Berlin, Erich Schmidt, 2005
Löffler2011	Löffler, Helge [Hrsg.]: Handbuch zum Internen Kontrollsystem: Anforderungen anhand des Jahresabschlusses und organisatorischen Aufbaus eines Unternehmens, Wien, Linde, 2011
Lück2006	Lück, Wolfgang; Bubendorfer, Reinhart: Zentrale Tätigkeiten der Internen Revision, Berlin, Erich Schmidt, 2006

Lück2009	Lück, Wolfgang; Albrecht, Tobias: Anforderungen an die Interne Revision, Berlin, Erich Schmidt, 2009
Maier2006	Maier, Claudia: Aufbau und Dokumentation interner Kontrollsysteme, Wien, Hochschulschriften: Wien, Wirtschaftsuniv. Dipl.-Arb., 2006
Menzies2004	Menzies, Christof [Hrsg.]: Sarbanes-Oxley Act professionelles Management interner Kontrollen, Stuttgart, Schäffer-Poeschel, 2004
Moeller2011	Moeller, Robert R.: COSO enterprise risk management establishing effective governance, risk, and compliance processes, Hoboken NJ [u.a.], Wiley, 2011
Moeller2014	Moeller, Robert R.: Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework, Hoboken, NJ [u.a.], Wiley, 2014 (e-book)
Peemöller2010	Peemöller, Volker H.; Kregel, Joachim: Grundlagen der Internen Revision, Berlin, Schmidt, 2010
Petsche2012	Petsche, Alexander [Hrsg.]: Handbuch Compliance: Bewusstseinsbildung für Compliance; Implementierung von Compliance-Systemen; Internal Investigations; inklusive Checklisten & Praxisbeispielen, Wien, LinkLexisNexis-Verl. ARD Orac , 2012
Pickett2010	Pickett, Spencer K H: The internal auditing Handbook, Chichester (u.a.), Wiley, 2010
Ramos2006	Ramos, Michael: How to comply with Sarbanes-Oxley section 404 assessing the effectiveness of internal control, Hoboken NJ, Wiley, 2006
Romeike/Hager2009	Romeike, Frank; Hager, Peter: Erfolgsfaktor Risiko-Management 2.0: Methoden, Beispiele, Checklisten - Praxishandbuch für Industrie und Handel, 2. Auflage, Wiesbaden, Gabler, 2009

Root1998	Root, Steven J.: Beyond COSO: internal control to enhance corporate governance, New York NY [u.a.], Wiley, 1998
Sommer2010	Sommer, Katerina: Risikoorientiertes Zusammenwirken der Internal Control, des Risikomanagements, des Internen Audits und der Externen Revision: theoretische Analyse, konzeptionelle Ansätze und praktische Gestaltung, St. Gallen, Hochschulschrift: St. Gallen, Univ. Diss., 2010
Sonnelitter2009	Sonnelitter, Robert J.: SOX 404 for Small Publicly Held Companies, Illinois, CCH, 2009
Steckel2007	Steckel, Rudolf: Aktuelle Entwicklungen und Herausforderungen der Internen Revision, Wien, Linde, 2007
Stelling2005	Stelling, Johannes N.: Kostenmanagement und Controlling, 2. überarbeitete Auflage, München; Wien, Oldenbourg, 2005
Stimson2006	Stimson, William A.: ISO 9001 and Sarbanes-Oxley - A System of Governance, Richmond, Paton Press LLC, 2006
Welge2012	Welge, Martin K.; Eulerich, Marc: Corporate - Governance - Management: Theorie und Praxis der guten Unternehmensführung, Wiesbaden, Gabler, 2012

Internetquellen

AAA1998-2014/About	http://aaahq.org/about.cfm, verfügbar am 31.07.2014, 16:22
AAA1998-2014/Join	http://aaahq.org/join.cfm, verfügbar am 31.07.2014, 16:22
AAA1998-2014/Statement of Responsibilities	http://aaahq.org/about/SOR.pdf, verfügbar am 31.07.2014, 14:56
ACFE2014/Fraud Tree	http://www.acfe.com/fraud-tree.aspx, verfügbar am 11.11.2014, 15:32
AICPA2006-2014/About	http://www.aicpa.org/About/Pages/About.aspx, verfügbar am 31.07.2014, 11:23
AICPA2010/History	http://www.aicpa.org/About/MissionandHistory/Pages/History%20of%20the%20AICPA.aspx, verfügbar am 01.08.2014, 09:16
CICA2013	http://www.cica.ca/about-cica/index.aspx, verfügbar am 31.05.2014, 17:11
COSO.org06/2013	http://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf, verfügbar am 27.12.2013, 12:35
COSO.org11/2010	http://www.coso.org/documents/COSOReleaseNov2010_000.pdf, verfügbar am 03.11.2014, 10:31
COSOERM2004	http://www.coso.org/documents/coso_erm_executivesummary.pdf, verfügbar am 11.11.2014, 17:12

Ecgi1992/Financial Aspects of Corporate Governance	http://www.ecgi.org/codes/documents/cadbury.pdf, verfügbar am 01.06.2014, 12:00
FEI2014/About	http://www.financialexecutives.org/KenticoCMS/about/about.aspx, verfügbar am 01.08.2014, 11:28
FEI2014/History	http://www.financialexecutives.org/KenticoCMS/About/History.aspx, verfügbar am 01.08.2014, 11:27
IIA2013/Standards-Guidance	https://global.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20German.pdf, verfügbar am 14.07.2014, 11:50
IIA2013/The Three Lines of Defense	https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf, verfügbar am 14.07.2014, 12:56
IIA2014/About	https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx, verfügbar am 01.08.2014, 12:47
IIA2014/Certification	https://na.theiia.org/certification/Pages/Certification.aspx, verfügbar am 01.08.2014, 12:50
IIA2014/Frequently Ask Questions	https://global.theiia.org/about/about-internal-auditing/Pages/Frequently-Asked-Questions.aspx, verfügbar am 14.07.2014, 10:35
IIA2014/Standards-and-Guidance	https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx, verfügbar am 01.08.2014, 12:48
IMA1997-2014/History	http://www.imanet.org/about_ima/our_history.aspx, verfügbar am 01.08.2014, 11:50

IMA1997-2014/Mission	http://www.imanet.org/about_ima/our_mission.aspx, verfügbar am 01.08.2014, 11:51
iso.org/About ISO	http://www.iso.org/iso/home/about.htm, verfügbar am 31.05.2014, 12:26
iso.org/Benefits Of ISO Standard	http://www.iso.org/iso/home/standards/benefitsofstandards.htm, verfügbar am 31.05.2014, 11:02
iso.org/The ISO Story	http://www.iso.org/iso/home/about/the_iso_story.htm#21, verfügbar am 31.05.2014, 12:19
KPMG26_2013/05	http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Newsletters/Defining-Issues/Documents/Defining-Issues-O-1305-26.pdf, verfügbar am 04.11.2014, 16:21
PCAOB2003-2014	http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2.aspx, Verfügbar am: 19.05.2014; 16:38
SOX2002	http://www.sec.gov/about/laws/soa2002.pdf, verfügbar am 29.05.2014, 11:18

Zeitschriftenartikel

CFOaktuell2010_25	Kreuzer, Christian: IKS - Internes Kontrollsystem, Wien, Linde CFO aktuell 2010 - 25, 2010
CFOaktuell2013_96	Busch, Jorg / Hjertonsson, Sofia: Sieben Elemente eines effizienten und wirksamen Compliance-Management-Systems - Kultur - Ziele - Risikoidentifizierung/-bewertung - Programm - Organisation - Kommunikation/Schulung - Überwachung/Verbesserung, Wien, Linde CFO aktuell 2013 - 96, 2013

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Wien, den 20. November 2014

Julia Lutz